



Manafort Home for nearly nine months and has failed to return all non-responsive material seized to Mr. Manafort.

## **I. DISCUSSION**

On the morning of July 26, 2017, agents entered the Manafort's home located in a condominium building. Once inside, the agents seized or imaged every electronic device and storage device in the home.

### **a. The Search Warrant was unconstitutionally overbroad**

The Search Warrant was fatally overbroad because it allowed the searching agents to indiscriminately seize records, emails, photographs and electronic devices from the Manafort Home. The Fourth Amendment does not permit the warrant that was issued in this case, which was essentially a general warrant for "any and all" financial documents and electronic devices. Rather, the Fourth Amendment requires that search warrants "'particularly describ[e] the place to be searched, and the persons or things to be seized," which operates to "prevent[ ] the seizure of one thing under a warrant describing another.'" *Jones v. Kirchner*, 835 F.3d 74, 79 (D.C. Cir. 2016) (quoting *Marron v. United States*, 275 U.S. 192, 195–96 (1927)).

The Search Warrant here fell short of the constitutional requirements set out above. For offenses occurring on or after January 1, 2006,<sup>3</sup> the Search Warrant directed the seizure of, *inter alia*, "[a]ny and all financial records for Paul Manafort, Jr., Kathleen Manafort, Richard Gates, or companies associated with Paul Manafort, Jr., Kathleen Manafort, or Richard Gates", (*see* Search Warrant, Attachment B, ¶ 1a.), "[e]vidence indicating Manafort's state of mind as it relates to the crimes under Investigation" (*id.* ¶ 1i.), and "[c]omputers or storage media used as a means to commit the Subject Offenses," (*id.* ¶ 2.).

---

<sup>3</sup> This crucial temporal limitation was missing from the search warrant for the storage unit.

A search warrant for “any and all financial records” of everyone residing at the subject location is exceptionally broad; indeed, nothing in the affidavit justifies so broad a warrant. And a warrant directing agents to seize all evidence of the subject’s “state of mind” does not restrict the agent’s discretion at all. Indeed, the warrant may just as well have told agents to search for and seize any evidence that the subject committed the subject offenses – all of which require knowledge and intent. While seizing agents naturally look for evidence of the subject’s guilt, the role of the warrant is to *limit* their discretion to determine what constitutes such evidence. This warrant did no such thing. Finally, the warrant allowed the agents to search for and seize any “computers or storage media” that may have been used in the “subject offenses,” but it did not limit the agents’ discretion in determining what computers or what storage media fit that description.

Recently, the D.C. Circuit Court of Appeals found wanting a similar warrant authorizing the seizure of all electronic devices. In *United States v. Griffith*, 867 F.3d 1265 (D.C. Cir. 2017), the appellate court invalidated a search and seizure warrant that “authorized the wholesale seizure of all electronic devices discovered in the apartment, including items owned by third parties.” *Id.* at 1270-71. In this case, the warrant authorized such a seizure.

Nor can the affidavit submitted by the FBI in support of the search warrant application (the “FBI Affidavit”)<sup>4</sup> save this defective warrant. The Supreme Court has made clear that the Fourth Amendment’s particularity requirements must be satisfied “in the warrant, *not in the supporting documents.*” *Groh v. Ramirez*, 540 U.S. 551, 557 (2004) (emphasis added). A court may only “construe a warrant with reference to a supporting application or affidavit if the warrant uses appropriate words of incorporation, and if the supporting document accompanies the warrant.” *Id.*

---

<sup>4</sup> A redacted copy of the FBI Affidavit is annexed hereto as Exhibit B.

at 557–58. The D.C. Circuit has recently explained that it will “read warrants by reference to an affidavit, [but], only if the issuing judge uses explicit words on the warrant indicating an intention to incorporate the affidavit’s contents and thereby limit [the warrant’s] scope.” *Griffith*, 867 F.3d 1265 at 1277. Here, the Search Warrant did not incorporate the FBI Affidavit.

**b. The FBI Affidavit failed to establish probable cause that the electronic devices had any connection to the subject offenses and would be found in the Manafort Home.**

As in *Griffith*, the search warrant affidavit in this case goes on at length about evidence of the subject’s purported involvement in the offenses. That exposition, however, is directed at establishing why there is reason to believe that an offense was committed and that the subject was the one who committed it. Importantly, an affidavit must also establish a reason to believe that the evidence sought will be found in the place to be searched. “Regardless of whether an individual is validly suspected of committing a crime, an application for a search warrant concerning his property or possessions must demonstrate cause to believe that evidence is likely to be found at the place to be searched.” *Griffith*, 867 F.3d at 1271 (internal quotation marks omitted).

An affidavit setting forth reasons to believe that an individual may have committed an offense, without more, is the proper basis of an arrest warrant—not a search warrant:

The Supreme Court has long distinguished between arrest warrants and search warrants. An arrest warrant rests on probable cause to believe that the suspect committed an offense; it thus primarily serves to protect an individual’s liberty interest against an unreasonable seizure of his person. A search warrant, by contrast, is grounded in probable cause to believe that the legitimate object of a search is located in a particular place. Rather than protect an individual’s person, a search warrant safeguards an individual’s interest in the privacy of his home and possessions against the unjustified intrusion of the police.

*Griffith*, 867 F.3d at 1271 (internal citations and quotation marks omitted).



In this case, the affidavit does not establish probable cause to believe that the electronic devices purportedly used in the commission of the subject offenses are likely to be found in the Manafort Home:

- One form in which the records might be found is data stored on a computer's hard drive or other storage media. (Search Warrant Affidavit ¶ 75 (footnote omitted).)
- In a July 2017 interview, [redacted] advised the FBI that there is a Mac desktop computer on the desk in the office at the Subject Premises, which is used by Manafort. (*Id.* ¶ 76.)
- For a variety of reasons, copies of historical records and current records are also frequently stored on external hard drives, thumb drives, and magnetic disks. There is reasonable cause to believe such media may be contained in and among records of Manafort's business and financial activity at the Subject Premises. FBI interviews of [redacted] further confirm that Manafort has made widespread use of electronic media in the course of his business activity. (*Id.*)
- For example, [redacted] told the FBI that Manafort had a drawer full of phones and electronic equipment at his old residence in Mount Vernon Square. At one point, Manafort gave [redacted] a bag of computers and directed [redacted] to have the drives wiped before giving them to charity. Manafort also gave [redacted] several additional devices, both laptops and cellular phones. (*Id.*)

Far from establishing that electronic devices purportedly used to commit the subject offenses are likely to be found in the Manafort Home, the affidavit offers the issuing magistrate nothing more than an affirmation that 1) generally speaking, computer hard drives and external storage media contain data; 2) there is an Apple McIntosh computer in the residence that Mr. Manafort uses for *some* purpose; 3) data is commonly stored on electronic media and Mr. Manafort has used electronic media in his business; and 4) at his previous residence, Mr. Manafort had what amounts to a junk drawer where he kept his old phones and other electronic devices before donating them to charity. These statements are an assortment of truisms; this recitation does not begin to establish "a nexus . . . between the item to be seized and criminal behavior." *Griffith*, 867 F.3d at 1271.

The affidavit is so lacking in probable cause to believe that electronic devices used in the alleged commission of the subject offenses would be found in the Manafort Home that no reasonable agent could have relied on it. Indeed, the *Griffith* court summed up the analysis as follows:

As the Court explained in *Leon*, the good-faith exception does not apply if a warrant is based on an affidavit so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable. When applying that standard, we consider the objective reasonableness not only of the officers who eventually executed the warrant, *but also of the officers who originally obtained it* or who provided information material to the probable-cause determination. We thus ask whether an objectively reasonable officer could think the affidavit established probable cause, keeping in mind the inadequacy of a bare bones affidavit.

*Griffith*, 867 F.3d at 1278 (internal citations and quotation marks omitted) (emphasis added). No reasonable agent could have believed that his affidavit established probable cause, and no executing agent could have believed it either. For this reason, the electronic evidence seized from the Manafort Home must be suppressed.

**c. The executing agents improperly seized materials beyond the warrant's scope**

Even where the particularity requirement is satisfied – and here it was not – “the search itself must be conducted in a reasonable manner, appropriately limited to the scope and intensity called for by the warrant.” *United States v. Heldt*, 668 F.2d 1238, 1256 (D.C. Cir. 1981) (citation and footnotes omitted). As the court in *Heldt* further explained:

When investigators fail to limit themselves to the particulars in the warrant, both the particularity requirement and the probable cause requirement are drained of all significance as restraining mechanisms, and the warrant limitation becomes a practical nullity. Obedience to the particularity requirement both in drafting and executing a search warrant is therefore essential to protect against the centuries-old fear of general searches and seizures.

*Id.* at 1257. In light of these principals, “the Fourth Amendment confines an officer executing a search warrant strictly within the bounds set by the warrant[.]” *Id.* at 1260 (quoting *Bivens v. Six*

*Unknown Named Agents*, 403 U.S. 388, 394 n.7 (1971)). Therefore, “in general, only items particularly mentioned in the warrant may be seized.” *Id.* at 1268 (collecting cases).

The agents that executed the Search Warrant in this case ran afoul of the above principles and seized every electronic and media device in the Manafort Home. For example, the search warrant inventory of electronic devices seized or imaged includes things such as an Apple iPod music device and some Apple iPod Touch music and video devices. No agent could have reasonably believed that he was seizing electronic devices used in the commission of the subject offenses.

**d. The government’s nearly nine-month retention of every item it seized constitutes an unreasonable search and seizure in violation of Mr. Manafort’s Fourth Amendment rights**

The FBI searched the Manafort Home more than eight months ago. To date, the government has not represented that the materials seized were subject to any process or procedure to insure the government only retained materials within the *scope* of the search warrant. The government has only represented that the materials have been subject to a *privilege* review. The government is required to review seized materials and “identify and return those materials not covered by the warrant.” *United States v. Soliman*, 2008 WL 4757300, at \*8 (W.D.N.Y. Oct. 29, 2008); *see also United States v. Tamura*, 694 F.2d 591, 597-98 (9th Cir. 1982) (holding the government’s retention of material outside the scope of the warrant was an “unconstitutional manner of executing the warrant”); *United States v. Comprehensive Drug Testing, Inc.*, 621 F.3d 1162, 1171 (9th Cir. 2010) (finding the government may only retain material seized from electronic systems if it was specified in the search warrant); *Doane v. United States*, 2009 WL 1619642, at \*10 (S.D.N.Y. June 5, 2009) (“[P]ermitting the Government to retain items outside

the scope of the warrant . . . would dramatically dilute the right to privacy in one's personal papers.”).

The first indictment in this matter was returned over five months ago, yet the government has made no indication that all of the materials seized have been reviewed for responsive documents and data. Moreover, the government has not identified materials that were seized even though they were outside the scope of the Search Warrant. As one court has explained, this alone violates the requirements of the Fourth Amendment. *See United States v. Metter*, 860 F. Supp. 2d 205 (E.D.N.Y. 2012). In *Metter*, the court granted the defendant's motion to suppress in light of the government's failure to identify seized documents responsive to a search warrant despite having fifteen months following the search to do so. *Id.* at 215. The court observed that “[t]he government's retention of *all* imaged electronic documents, including personal emails, without *any* review whatsoever to determine not only their relevance to this case, but also to determine whether any recognized legal privileges attached to them, is unreasonable and disturbing.” *Id.* (emphasis in original). *See also United States v. Debbi*, 244 F. Supp. 2d 235, 238 (S.D.N.Y. 2003) (failure to review search material for eight months violated the Fourth Amendment). As individuals and businesses become ever more reliant on computers and other electronic devices, federal courts have become increasingly concerned that the government's ability to seize entire hard drives for off-site examinations not “become a vehicle” for plainly unconstitutional “general” searches. *Comprehensive Drug Testing, Inc.*, 621 F.3d at 1177; *see also United States v. Wey*, 256 F. Supp. 3d 355, 406-07 (S.D.N.Y. 2017) (granting motion to suppress).

Even if the government had completed its review of the materials seized within a reasonable time period in this case – which it has not – courts require that, once the government completes its review, it must return all non-responsive information which “it ha[d] no probable

cause to collect” in the first place. *See, e.g., Comprehensive Drug Testing*, 621 F.3d at 1177; *see also Tamura*, 694 F.2d at 596-97 (retention of “documents not described in the warrant ... for at least six months after locating the relevant documents” was “an unreasonable and therefore unconstitutional manner of executing the warrant”). Without this requirement, the government’s practice of over-seizing documents for offsite review would lead to the indefinite retention of all hard copy documents and electronically-stored material, a clear violation of the Fourth Amendment. *See, e.g., Comprehensive Drug Testing*, 621 F.3d at 1176; *Metter*, 860 F. Supp. 2d at 216 (“[T]he Fourth Amendment would lose all force and meaning in the digital era and citizens will have no recourse as to the unlawful seizure of information that falls outside the scope of a search warrant and its subsequent dissemination.”).

In *United States v. Debbi*, the government obtained search warrants permitting seizure of items related to allegations of obstruction of justice and health care fraud. 244 F. Supp.2d at 236. Pursuant to those warrants, federal agents seized electronic and paper files, financial documents, and patient reports. Thereafter, the government failed to take any steps to separate seized documents that fell within the scope of the warrants from those clearly outside the scope. *Id.* at 237. The *Debbi* court found that the government “felt free to invade [the defendant’s] home, seize his records without meaningful limitation and restraint, pick over them for months thereafter without determining which were actually evidence of the alleged crimes, and even now refrain from returning what it was never entitled to seize.” *Id.* at 238. Thus, the court suppressed all seized materials that the government had not yet determined to be within the scope of the warrants. *Id.*

The result should be no different here, where the government executed the Search Warrant nearly nine months ago and, to date, the defense has no reason to believe that the material seized

from the Manafort Home has even been fully reviewed and where no material deemed unresponsive to the Search Warrant has been returned to Mr. Manafort.

Wherefore, Mr. Manafort respectfully moves the Court to suppress all evidence and fruits thereof relating to the government's search of the Manafort Home on the grounds stated herein.

Dated: April 9, 2018

Respectfully submitted,

/s/

Kevin M. Downing  
(D.C. Bar No. 1013984)  
Law Office of Kevin M. Downing  
601 New Jersey Avenue NW  
Suite 620  
Washington, DC 20001  
(202) 754-1992  
kevindowning@kdowninglaw.com

/s/

Thomas E. Zehnle  
(D.C. Bar No. 415556)  
Law Office of Thomas E. Zehnle  
601 New Jersey Avenue NW  
Suite 620  
Washington, DC 20001  
(202) 368-4668  
tezehnle@gmail.com

## UNITED STATES DISTRICT COURT

for the  
Eastern District of Virginia

In the Matter of the Search of  
(Briefly describe the property to be searched  
or identify the person by name and address)

Case No. 1:17SW449

THE PREMISES LOCATED [REDACTED]  
[REDACTED] ALEXANDRIA, VIRGINIA 22314

UNDER SEAL

## SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Eastern District of Virginia  
(identify the person or describe the property to be searched and give its location):

See Attachment A

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal (identify the person or describe the property to be seized):

See Attachment B

**YOU ARE COMMANDED** to execute this warrant on or before August 8, 2017 (not to exceed 14 days)  
☒ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to Honorable Theresa C. Buchanan  
(United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (check the appropriate box).

☐ for 7 days (not to exceed 30) ☐ until, the facts justifying, the later specific date of 11:25 am

Date and time issued:

7/25/17 11:25 am

/s/  
Theresa Carroll Buchanan  
United States Magistrate Judge  
Judge's signature

City and state:

Alexandria, Virginia

Honorable Theresa C. Buchanan

Printed name and title

**Return**

Case No.:

1:17SW449

Date and time warrant executed:

7/26/2017 4:56PM

Copy of warrant and inventory left with:

Paul Manafort

Inventory made in the presence of:

Paul Manafort

Inventory of the property taken and name of any person(s) seized:


See attached:


- List of items seized (Attachment A)
- List of items digitally imaged, not physically taken ~~seized~~<sup>BD</sup> (Attachment B)
- List of items seized, Flagged For possible attorney-client privilege (Attachment C)

**Certification**

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: 8/8/17

  
 Executing officer's signature

  
 Printed name and title

Special Agent



FD-697 (Rev 8-11-94)

Page 1 of 4

**Attachment A**

**UNITED STATE DEPARTMENT OF JUSTICE  
FEDERAL BUREAU OF INVESTIGATION**

Receipt for Property Received/Returned/Released/Seized

File #: 205B-WF-  
6832812

On (date) 7/26/2017

item(s) listed below were:

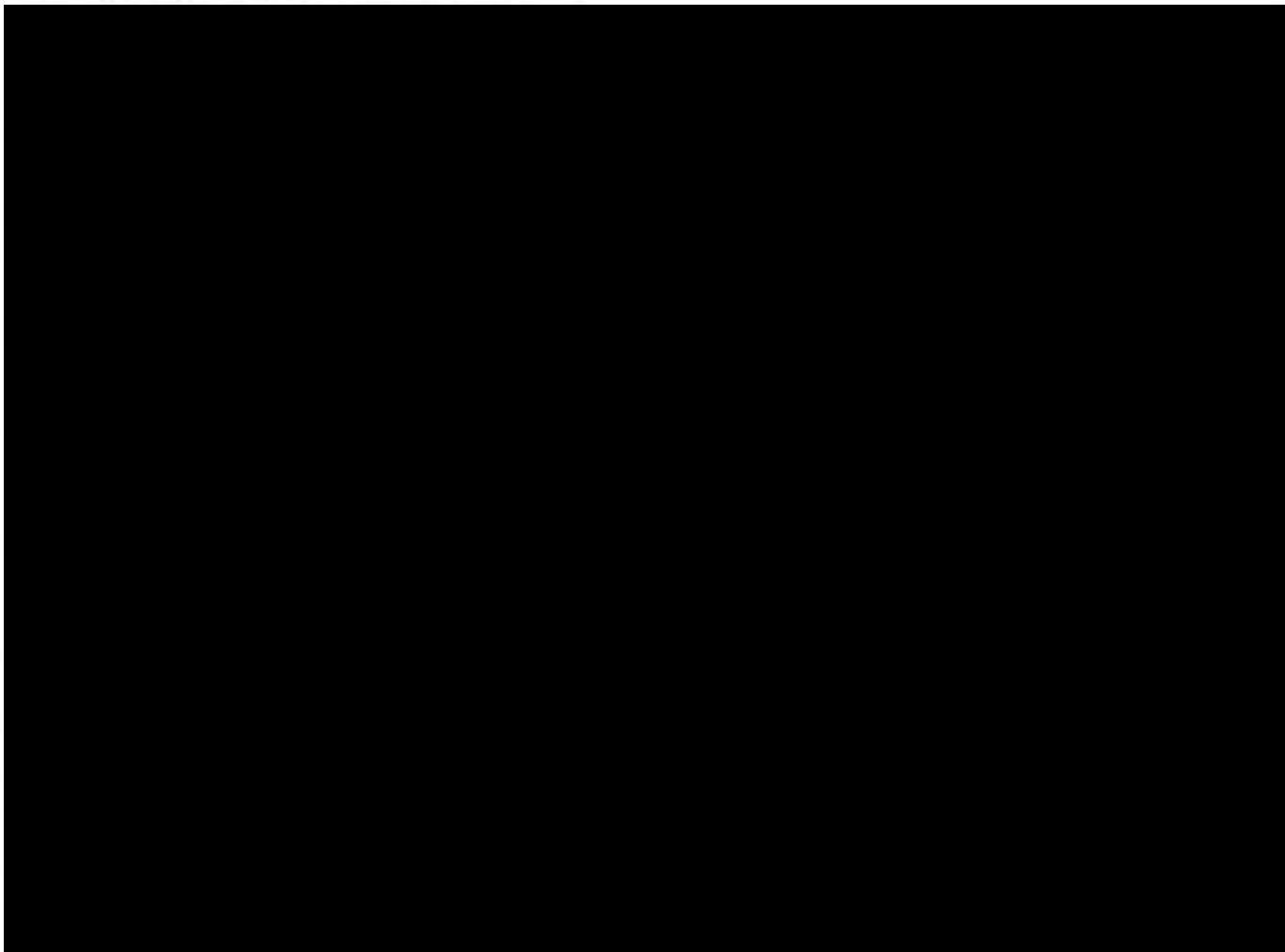
- ☐ Received From
- ☐ Received To
- ☐ Released To
- ☒ Seized

(Name) Paul Manafort

(Street Address) [REDACTED]

(City) Alexandria, VA 22314

Description of Item(s):



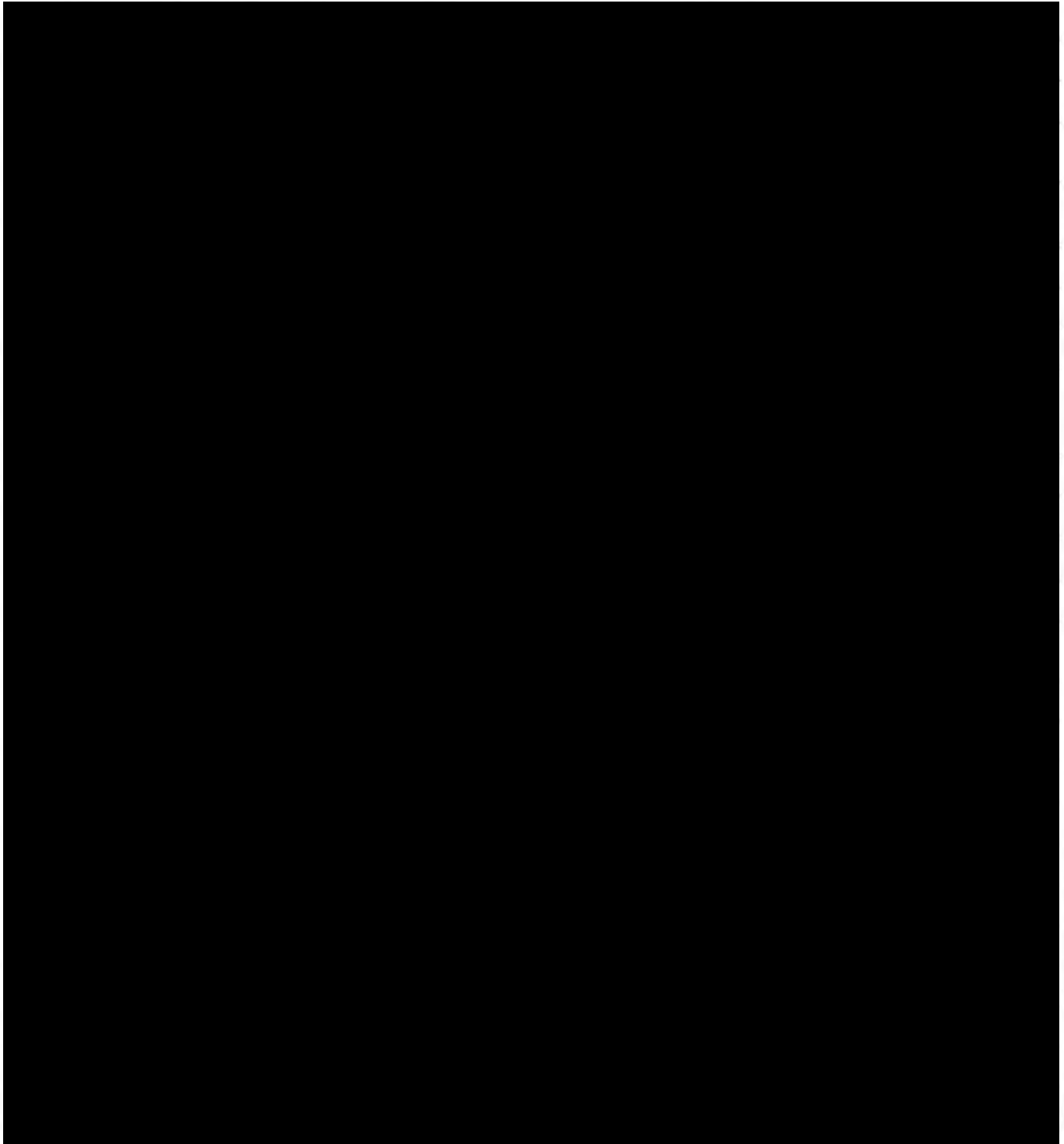
FD-597 (Rev 8-11-94)

Page 2 of 4

**UNITED STATE DEPARTMENT OF JUSTICE  
FEDERAL BUREAU OF INVESTIGATION**

Receipt for Property    Received/Returned/Released/Seized

File #: 205B-WF-  
6832812



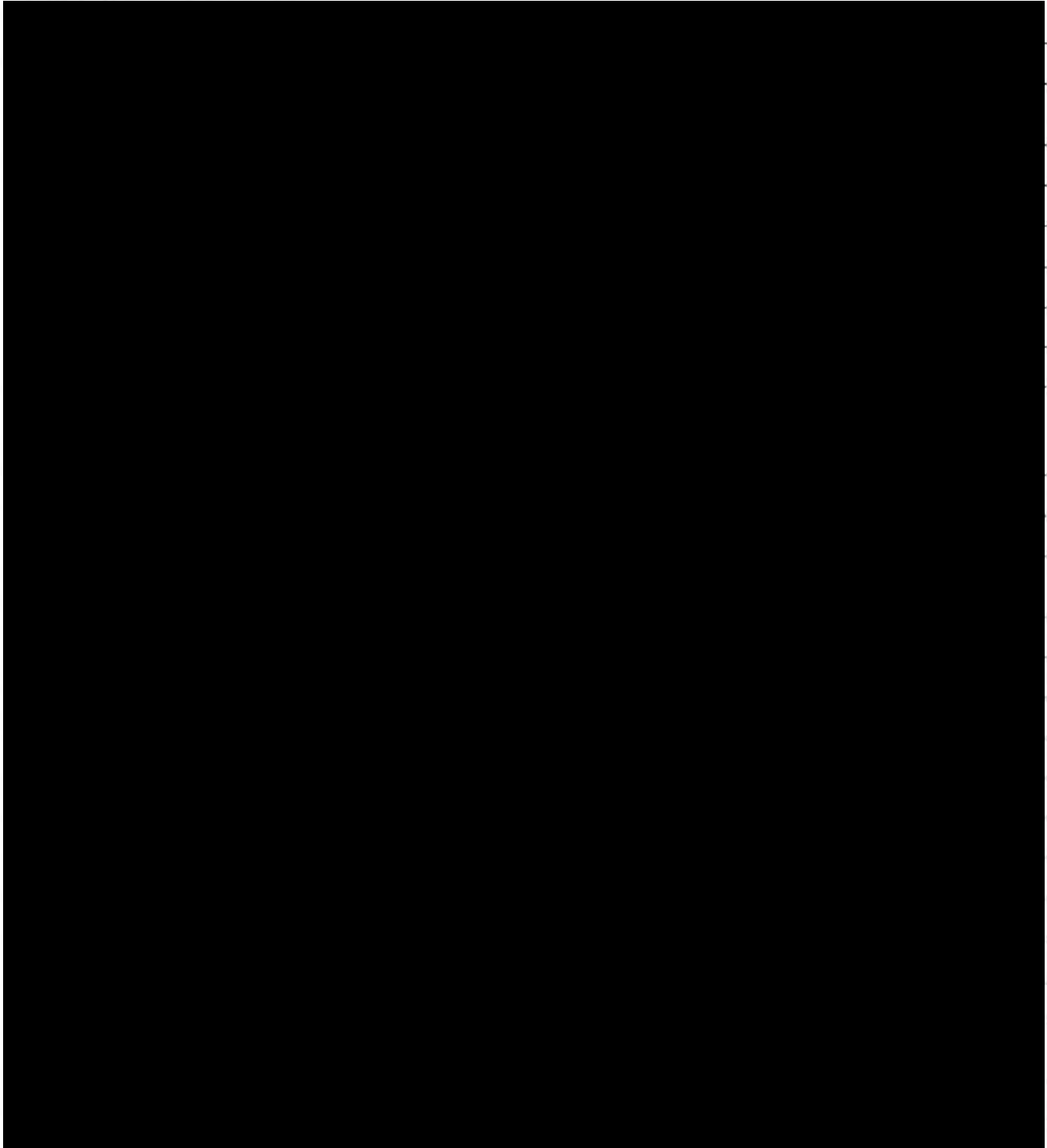
FD-597 (Rev 8-11-94)

Page 3 of 4

**UNITED STATE DEPARTMENT OF JUSTICE  
FEDERAL BUREAU OF INVESTIGATION**

Receipt for Property    Received/Returned/Released/Seized

File #: 205B-WF-  
6832812



Receipt for Property      Received/Returned/Released/Seized

**File #: 205B-WF-6832812**

Received By [REDACTED]

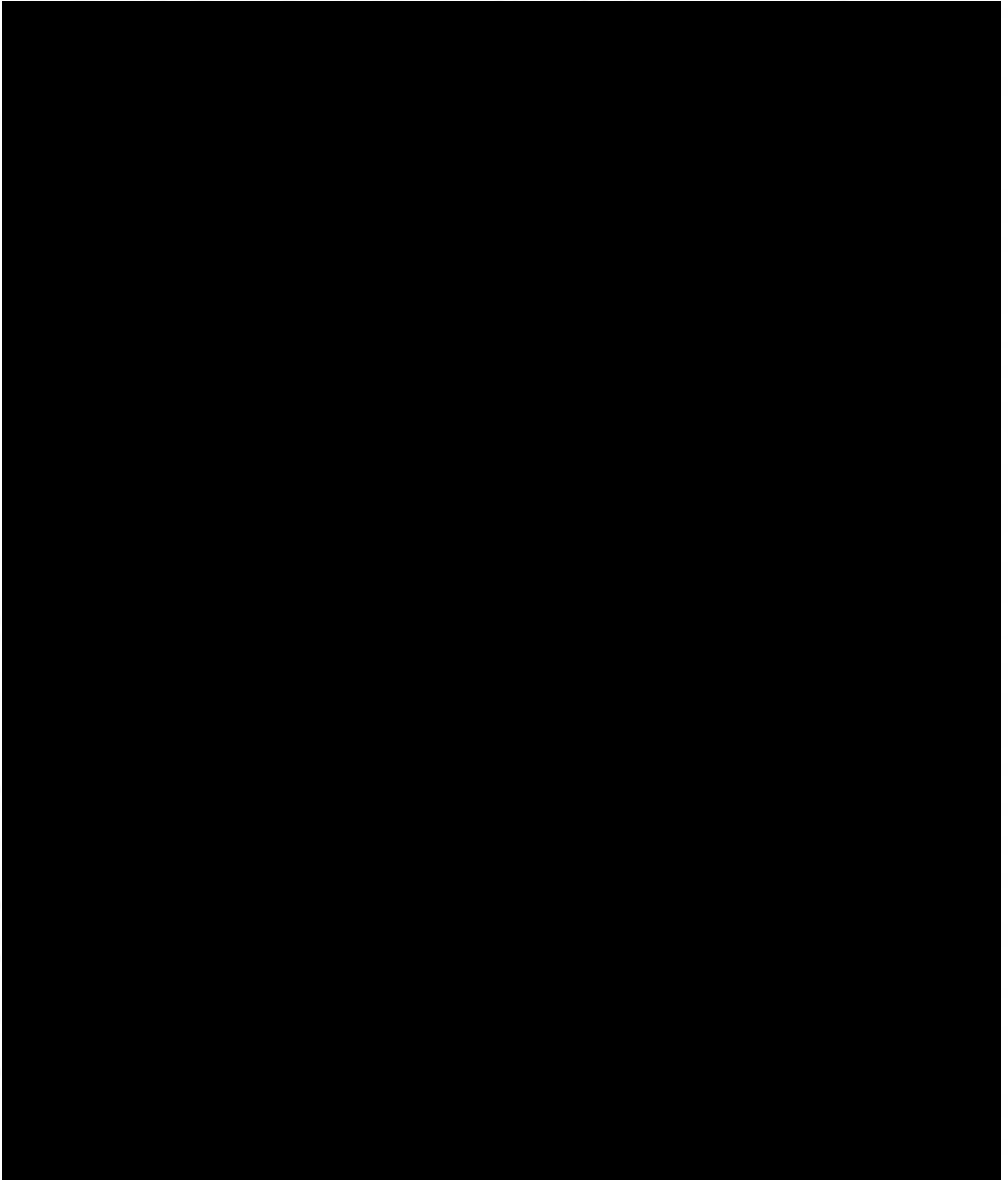
**Received From** Paul Manafort

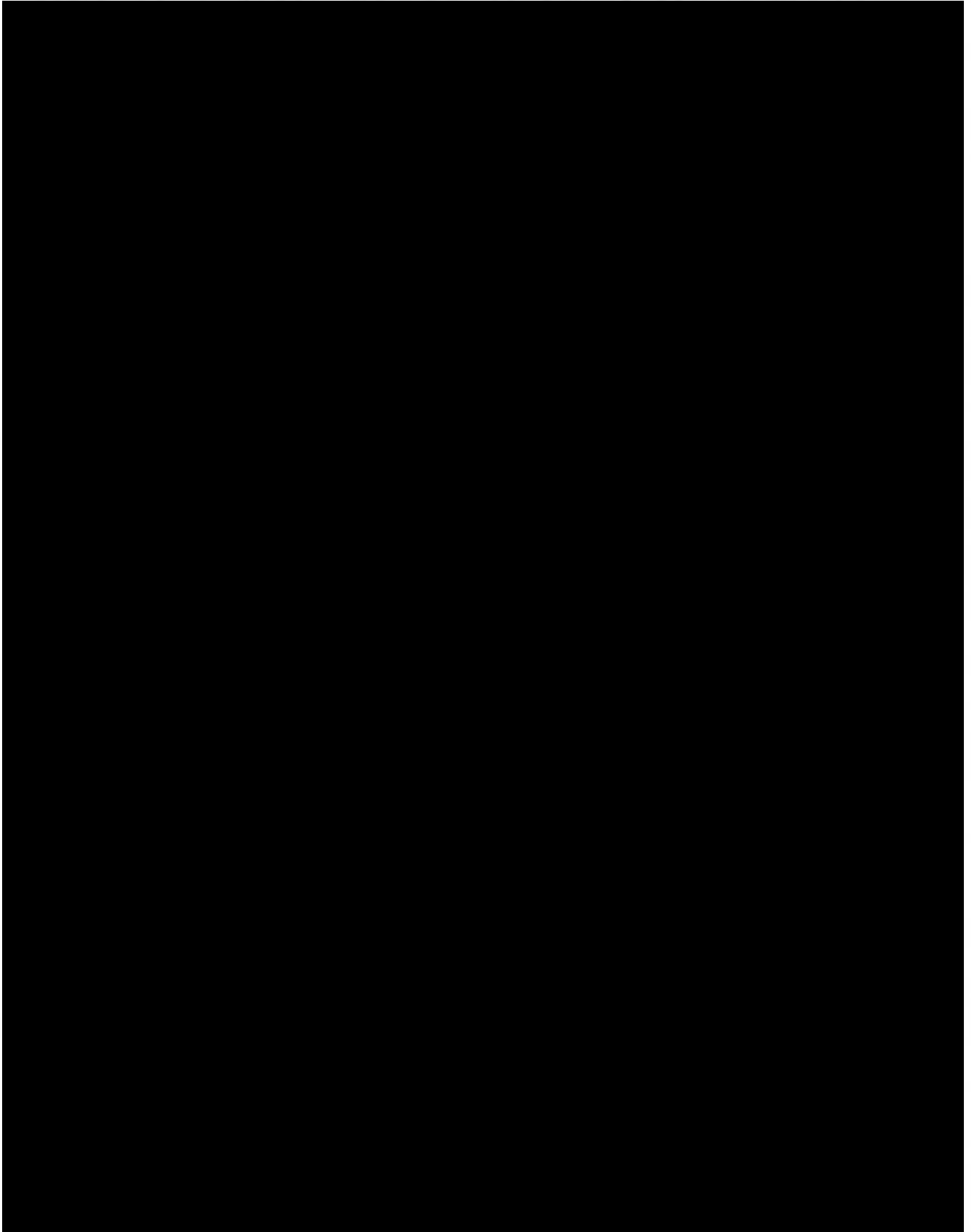
(signature) \_\_\_\_\_

(signature) \_\_\_\_\_

**ATTACHMENT B**

List of items digitally imaged on-premises, not physically taken:





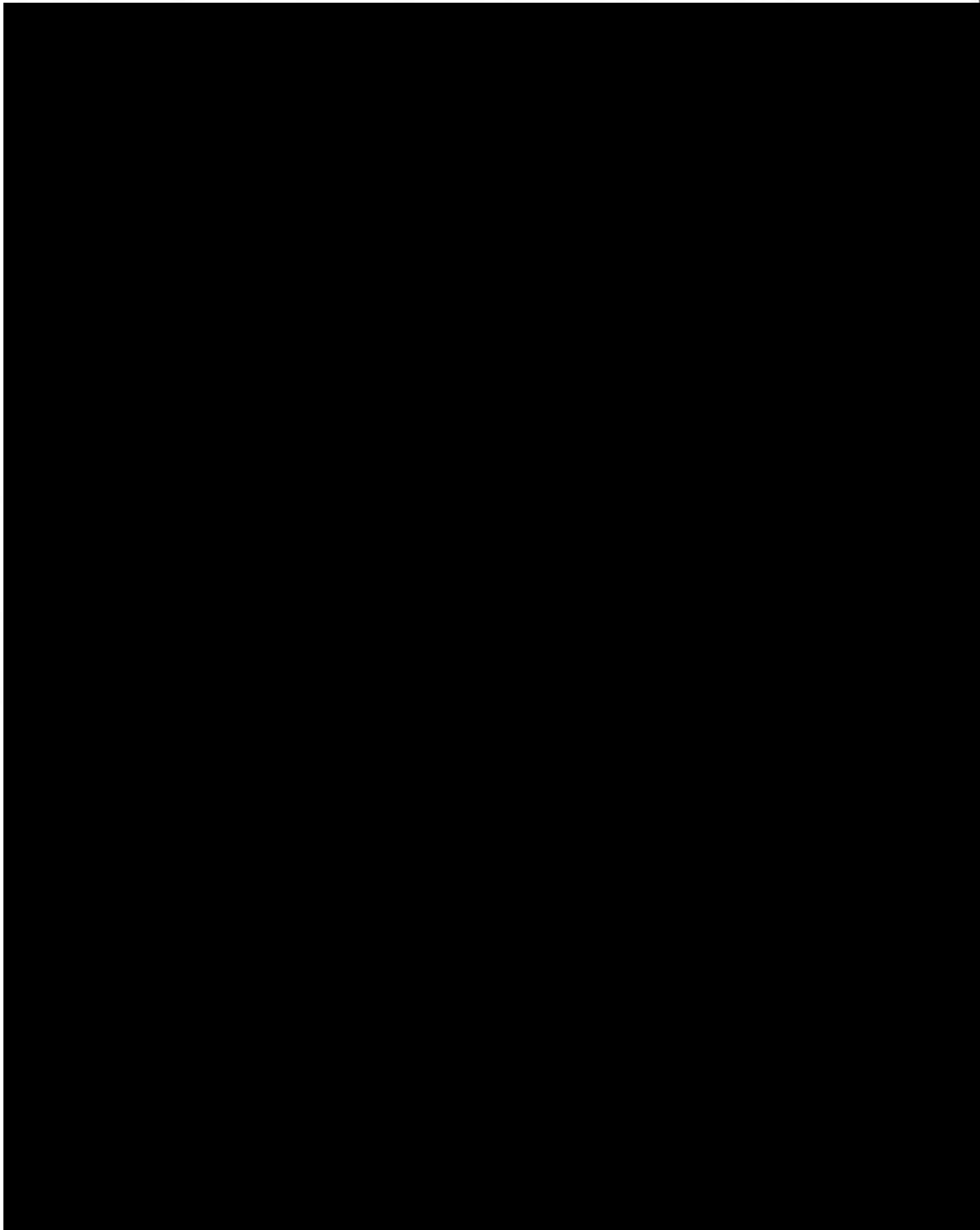


**Attachment C**

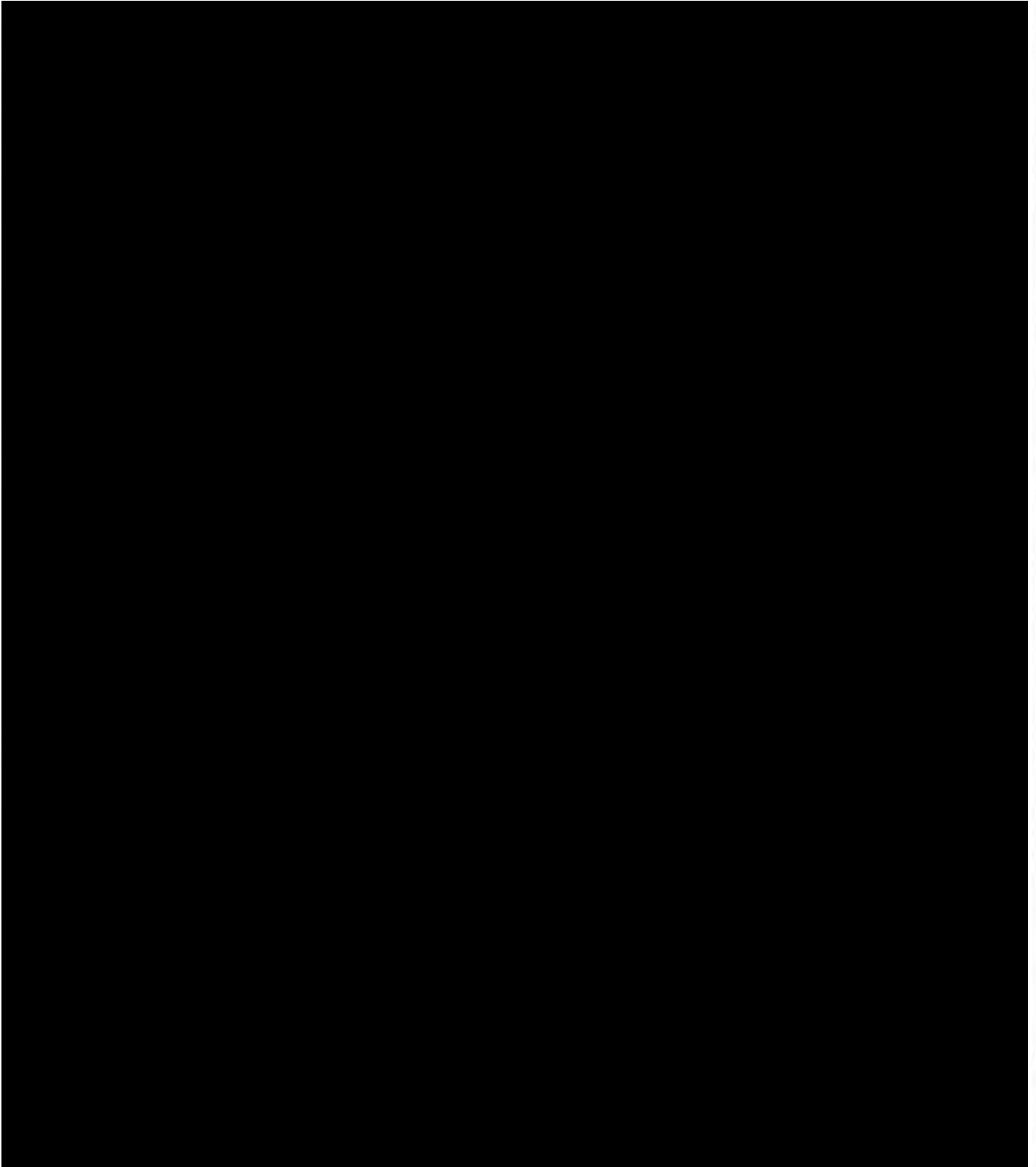
205B-WF-6032812

7/26/2017

collected item log - possible  
attorney client privilege







**ATTACHMENT A**

**The Property to Be Searched**

The premises to be searched (the "Subject Premises") is the condominium unit located at [REDACTED] Alexandria, VA 22314, including the storage unit numbered [REDACTED] as well as any locked drawers, containers, cabinets, safes, computers, electronic devices, and storage media (such as hard disks or other media that can store data) found therein.

**ATTACHMENT B**

**Items to Be Seized (or, in the alternative, identified)**

1. Records relating to violations of 31 U.S.C. §§ 5314, 5322(a) (failure to file a report of foreign bank and financial accounts); 22 U.S.C. § 611, *et. seq.* (foreign agents registration act); 26 U.S.C. § 7206(1) (filing a false tax return); 18 U.S.C. § 1014 (fraud in connection with the extension of credit); 18 U.S.C. §§ 1341, 1343, and 1349 (mail fraud, wire fraud, and conspiracy to commit these offenses); 18 U.S.C. §§ 1956 and 1957 (money laundering and money laundering conspiracy); 52 U.S.C. §§ 30121(a)(1)(A) and (a)(2) (foreign national contributions); and 18 U.S.C. §§ 371 and 2 (conspiracy, aiding and abetting, and attempt to commit such offenses) (collectively, the “Subject Offenses”), occurring on or after January 1, 2006, including but not limited to:

- a. Any and all financial records for Paul Manafort, Jr., Kathleen Manafort, Richard Gates, or companies associated with Paul Manafort, Jr., Kathleen Manafort, or Richard Gates, including but not limited to records relating to any foreign financial accounts and records relating to payments by or on behalf of any foreign government, foreign officials, foreign entities, foreign persons, or foreign principals;
- b. Any and all federal and state tax documentation, including but not limited to personal and business tax returns and all associated schedules for Paul Manafort, Jr., Richard Gates, or companies associated with Manafort or Gates;
- c. Letters, correspondence, emails, or other forms of communications with any foreign financial institution, or any individual acting as the signatory or controlling any foreign bank account;
- d. Records relating to efforts by Manafort, Gates, or their affiliated entities to conduct activities on behalf of, for the benefit of, or at the direction of any foreign government, foreign officials, foreign entities, foreign persons, or foreign principals, including but not limited to the Party of Regions and Viktor Yanukovich;
- e. Records relating to, discussing, or documenting Telmar Investments Limited, Tiakora Ventures Limited, Lucicle Consultants Limited, Actinet Trading Limited, Black Sea View Limited, Bletilla Ventures Limited, Evo Holdings Limited, Global Highway Limited, Leviathan Advisors Limited, Loav Advisors Limited, Peranova Holdings Limited, including but not limited to bank records, canceled checks, money drafts, letters of credit, cashier’s checks, safe deposit records, checkbooks, and check stubs, duplicates and copies of checks, deposit items, savings passbooks, wire transfer records, and similar bank and financial account records;
- f. Physical items purchased through the use of funds from Cypriot accounts, including but not limited to rugs purchased from J & J Oriental Rugs, a Bijan Black Titanium “Royal Way” watch, and clothing purchased from House of Bijan and Alan Couture;

- g. Evidence relevant to any false statements, pretenses, representations, or material omissions in connection with communications with the Department of Justice, the Internal Revenue Service, tax preparers, accountants, or banks;
  - h. Communications, records, documents, and other files involving any of the attendees of the June 9, 2016 meeting at Trump tower, as well as Aras and Amin Agalorov;
  - i. Evidence indicating Manafort's state of mind as it relates to the crimes under investigation;
  - j. The identity of any person(s)—including records that help reveal the whereabouts of the person(s)—who communicated with Manafort about any matters relating to activities conducted by Manafort on behalf of, for the benefit of, or at the direction of any foreign government, foreign officials, foreign entities, foreign persons, or foreign principals;
  - k. Any and all daily planners, logs, calendars, or schedule books relating to Manafort or Gates.
2. Computers or storage media used as a means to commit the Subject Offenses.
3. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):
- a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
  - b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
  - c. evidence of the lack of such malicious software;
  - d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;
  - e. evidence indicating the computer user's state of mind as it relates to the crime under investigation;
  - f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

- g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;
- h. evidence of the times the COMPUTER was used;
- i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
- j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
- k. records of or information about Internet Protocol addresses used by the COMPUTER;
- l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;
- m. contextual information necessary to understand the evidence described in this attachment.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

# UNITED STATES DISTRICT COURT

for the  
Eastern District of Virginia

**Under Seal**

JUL 25 2017

In the Matter of the Search of  
(Briefly describe the property to be searched  
or identify the person by name and address)

Case No. 1:17SW449

THE PREMISES LOCATED [REDACTED]  
[REDACTED] ALEXANDRIA, VIRGINIA 22314

## APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A

located in the Eastern District of Virginia, there is now concealed (identify the person or describe the property to be seized):

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section  
See attached Affidavit.

Offense Description

The application is based on these facts:  
See attached Affidavit.

☒ Continued on the attached sheet.

☐ Delayed notice of \_\_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Reviewed by AUSA/SAUSA:

[REDACTED]

Applicant's signature

Special Agent, FBI

Printed name and title

/s/

Theresa Carroll Buchanan  
United States Magistrate Judge

Judge's signature

The Honorable Theresa C. Buchanan

Printed name and title

Sworn to before me and signed in my presence.

Date: 07/25/2017

City and state: Alexandria, VA

**ATTACHMENT A**

**The Property to Be Searched**

The premises to be searched (the "Subject Premises") is the condominium unit located at [REDACTED] Alexandria, VA 22314, including the storage unit numbered [REDACTED], as well as any locked drawers, containers, cabinets, safes, computers, electronic devices, and storage media (such as hard disks or other media that can store data) found therein.



**ATTACHMENT B**

**Items to Be Seized (or, in the alternative, identified)**

1. Records relating to violations of 31 U.S.C. §§ 5314, 5322(a) (failure to file a report of foreign bank and financial accounts); 22 U.S.C. § 611, *et. seq.* (foreign agents registration act); 26 U.S.C. § 7206(1) (filing a false tax return); 18 U.S.C. § 1014 (fraud in connection with the extension of credit); 18 U.S.C. §§ 1341, 1343, and 1349 (mail fraud, wire fraud, and conspiracy to commit these offenses); 18 U.S.C. §§ 1956 and 1957 (money laundering and money laundering conspiracy); 52 U.S.C. §§ 30121(a)(1)(A) and (a)(2) (foreign national contributions); and 18 U.S.C. §§ 371 and 2 (conspiracy, aiding and abetting, and attempt to commit such offenses) (collectively, the "Subject Offenses"), occurring on or after January 1, 2006, including but not limited to:

- a. Any and all financial records for Paul Manafort, Jr., Kathleen Manafort, Richard Gates, or companies associated with Paul Manafort, Jr., Kathleen Manafort, or Richard Gates, including but not limited to records relating to any foreign financial accounts and records relating to payments by or on behalf of any foreign government, foreign officials, foreign entities, foreign persons, or foreign principals;
- b. Any and all federal and state tax documentation, including but not limited to personal and business tax returns and all associated schedules for Paul Manafort, Jr., Richard Gates, or companies associated with Manafort or Gates;
- c. Letters, correspondence, emails, or other forms of communications with any foreign financial institution, or any individual acting as the signatory or controlling any foreign bank account;
- d. Records relating to efforts by Manafort, Gates, or their affiliated entities to conduct activities on behalf of, for the benefit of, or at the direction of any foreign government, foreign officials, foreign entities, foreign persons, or foreign principals, including but not limited to the Party of Regions and Viktor Yanukovich;
- e. Records relating to, discussing, or documenting Telmar Investments Limited, Tiakora Ventures Limited, Lucicle Consultants Limited, Actinet Trading Limited, Black Sea View Limited, Bletilla Ventures Limited, Evo Holdings Limited, Global Highway Limited, Leviathan Advisors Limited, Loav Advisors Limited, Peranova Holdings Limited, including but not limited to bank records, canceled checks, money drafts, letters of credit, cashier's checks, safe deposit records, checkbooks, and check stubs, duplicates and copies of checks, deposit items, savings passbooks, wire transfer records, and similar bank and financial account records;
- f. Physical items purchased through the use of funds from Cypriot accounts, including but not limited to rugs purchased from J & J Oriental Rugs, a Bijan Black Titanium "Royal Way" watch, and clothing purchased from House of Bijan and Alan Couture;



- g. Evidence relevant to any false statements, pretenses, representations, or material omissions in connection with communications with the Department of Justice, the Internal Revenue Service, tax preparers, accountants, or banks;
  - h. Communications, records, documents, and other files involving any of the attendees of the June 9, 2016 meeting at Trump tower, as well as Aras and Amin Agalorov;
  - i. Evidence indicating Manafort's state of mind as it relates to the crimes under investigation;
  - j. The identity of any person(s)—including records that help reveal the whereabouts of the person(s)—who communicated with Manafort about any matters relating to activities conducted by Manafort on behalf of, for the benefit of, or at the direction of any foreign government, foreign officials, foreign entities, foreign persons, or foreign principals;
  - k. Any and all daily planners, logs, calendars, or schedule books relating to Manafort or Gates.
2. Computers or storage media used as a means to commit the Subject Offenses.
3. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):
- a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
  - b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
  - c. evidence of the lack of such malicious software;
  - d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;
  - e. evidence indicating the computer user's state of mind as it relates to the crime under investigation;
  - f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

- g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;
- h. evidence of the times the COMPUTER was used;
- i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
- j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
- k. records of or information about Internet Protocol addresses used by the COMPUTER;
- l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;
- m. contextual information necessary to understand the evidence described in this attachment.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

UNITED STATES DISTRICT COURT  
EASTERN DISTRICT OF VIRGINIA

Alexandria Division

JUL 25 2017

THE PREMISES LOCATED AT [REDACTED]  
[REDACTED] ALEXANDRIA,  
VIRGINIA 22314

Criminal No. 1:17-sw-449

Filed Under Seal

**AFFIDAVIT IN SUPPORT OF AN  
APPLICATION FOR A SEARCH WARRANT**

[REDACTED] Federal Bureau of Investigation ("FBI"), being duly sworn, deposes and says:

**I. Introduction**

**A. Affiant**

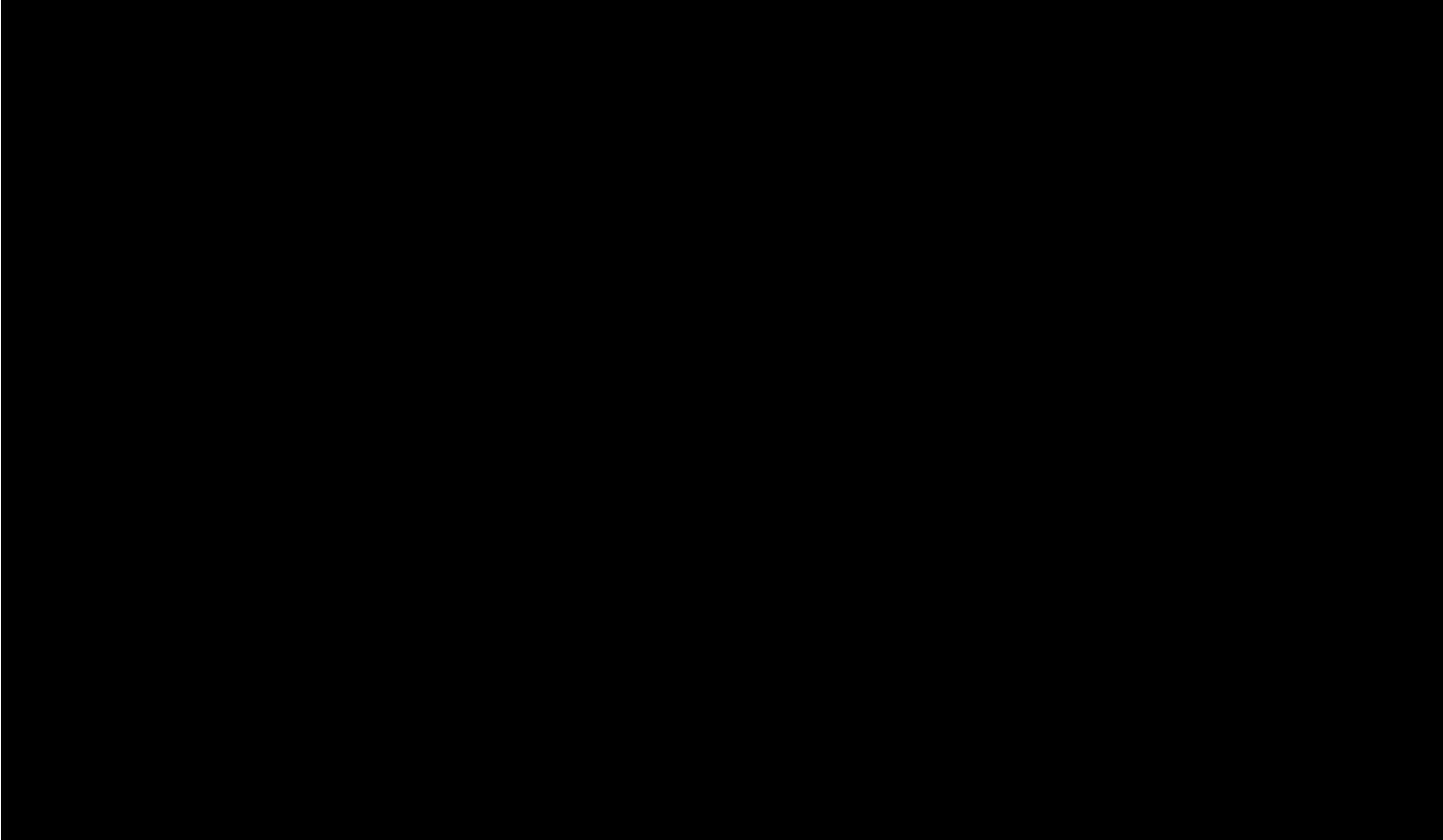
1. I am a Special Agent with the FBI and have been since 2015. I am currently assigned to the investigation being conducted by the Department of Justice Special Counsel. As a Special Agent of the FBI, I have received training and experience in investigating criminal and national security matters. Prior to my employment with the FBI, I spent seven years in the software industry and have extensive experience working with computer technology.

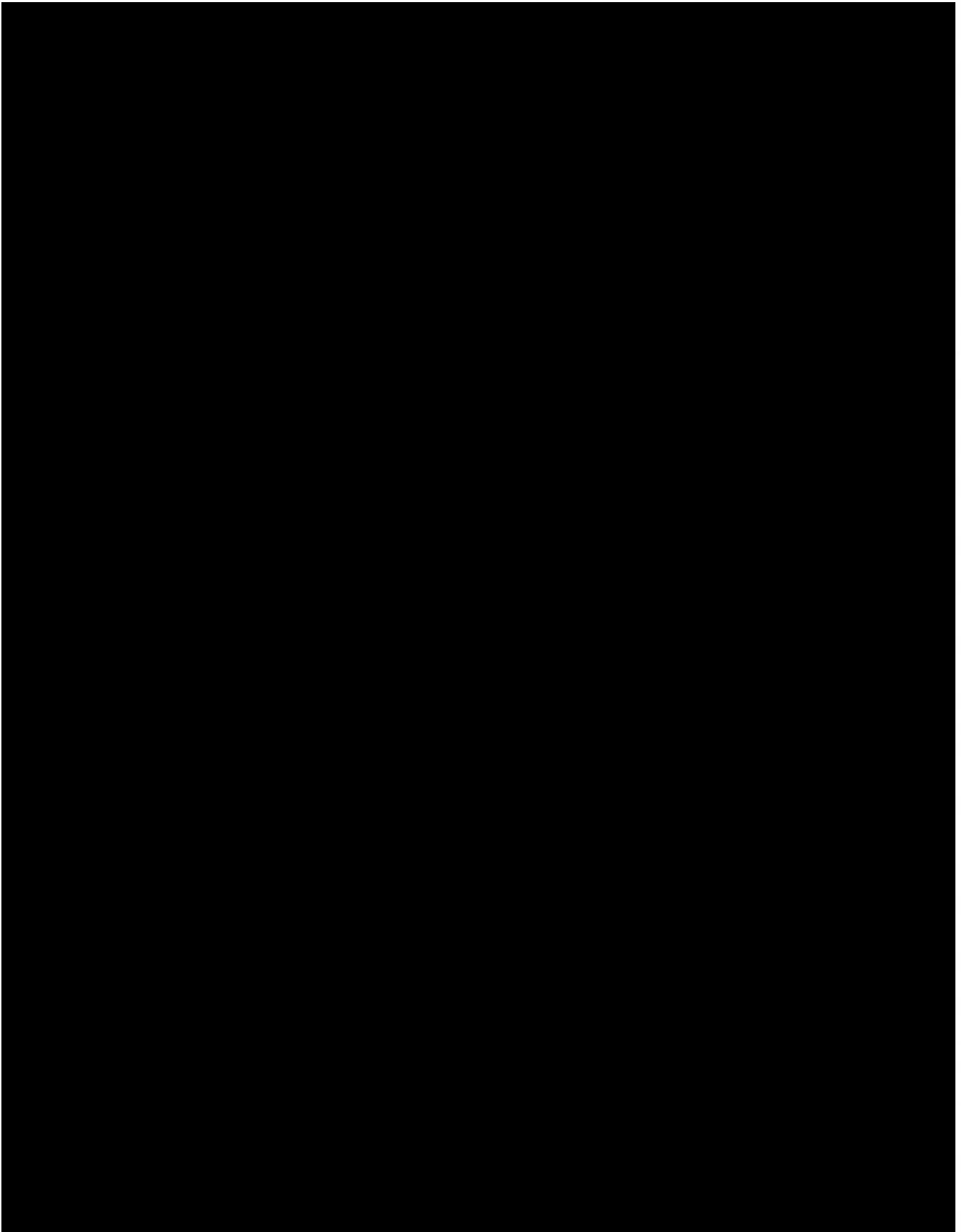
2. I make this affidavit in support of an application pursuant to Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises located at [REDACTED] Alexandria, Virginia 22314 (the "Subject Premises"), which is described more particularly in Attachment A, in order to locate and seize (and/or photograph) the items described in Attachment B. This affidavit is based upon my personal knowledge, my review of documents and other evidence, my conversations with other law enforcement personnel, and my training and experience. Because this affidavit is being submitted for the limited purpose of establishing probable cause, it does not include all the facts that I have learned during the course of my

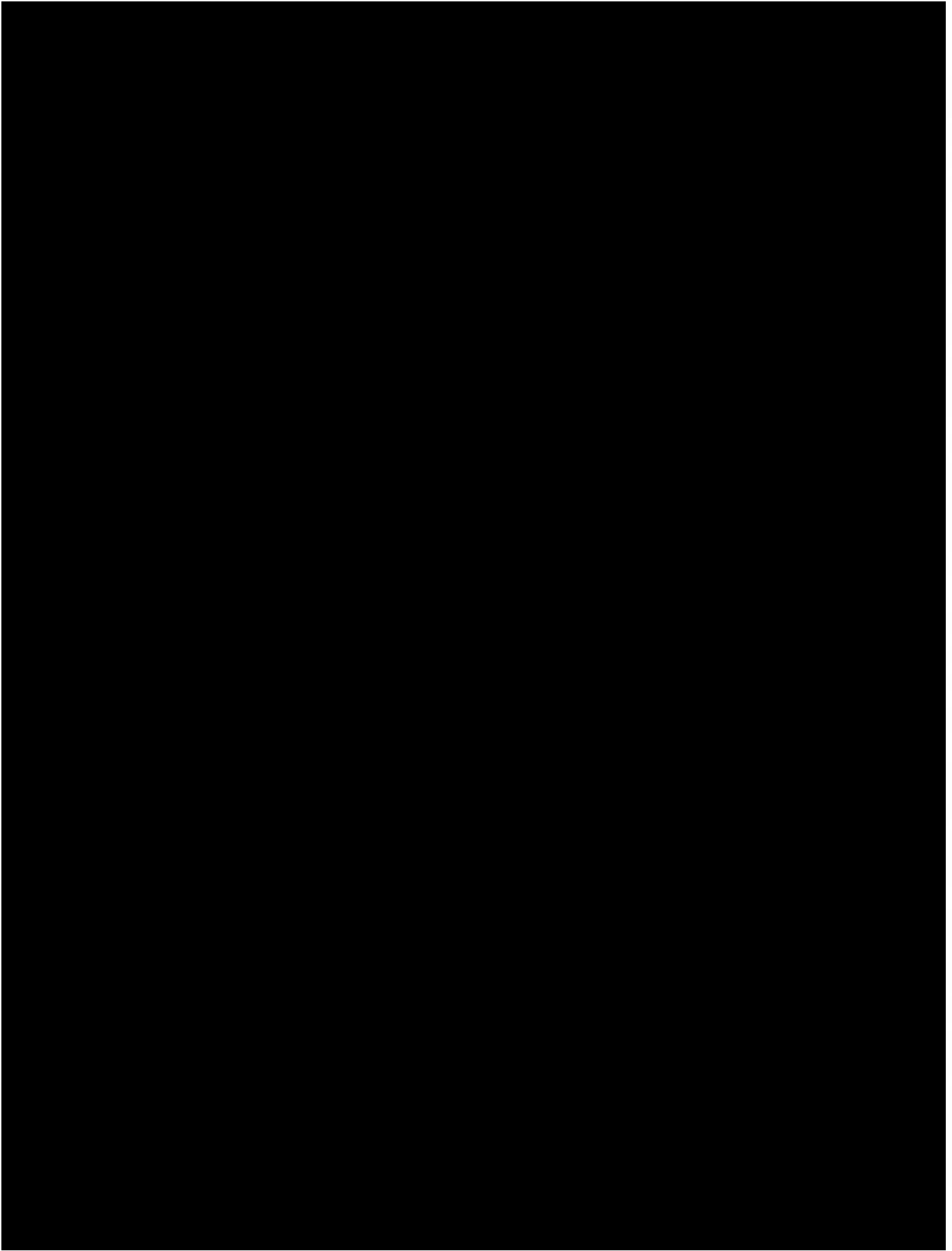
investigation. Where the contents of documents and the statements, and conversations of others are reported herein, they are reported in substance and in pertinent part, except where otherwise indicated.

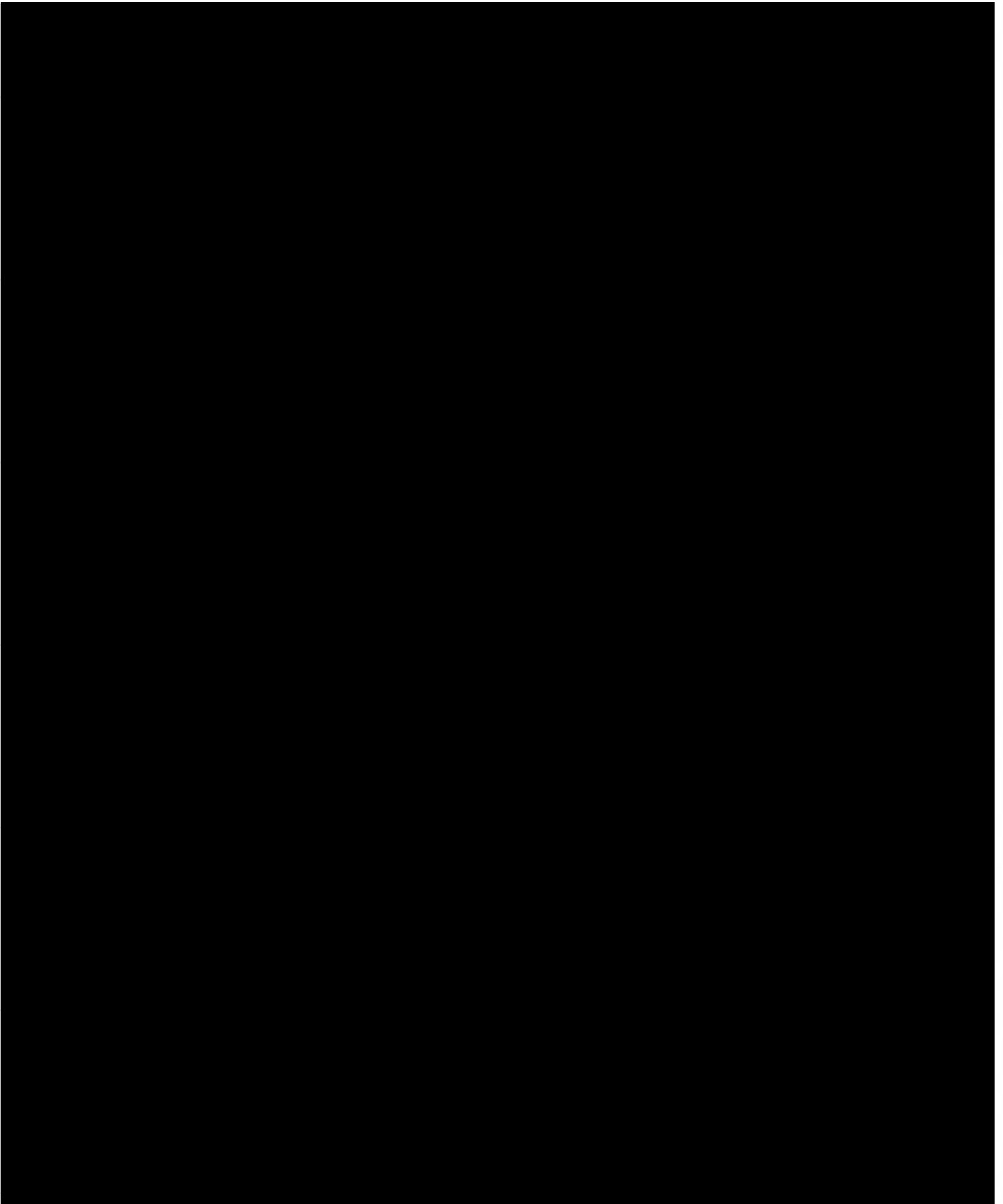
**B. The Subject Offenses**

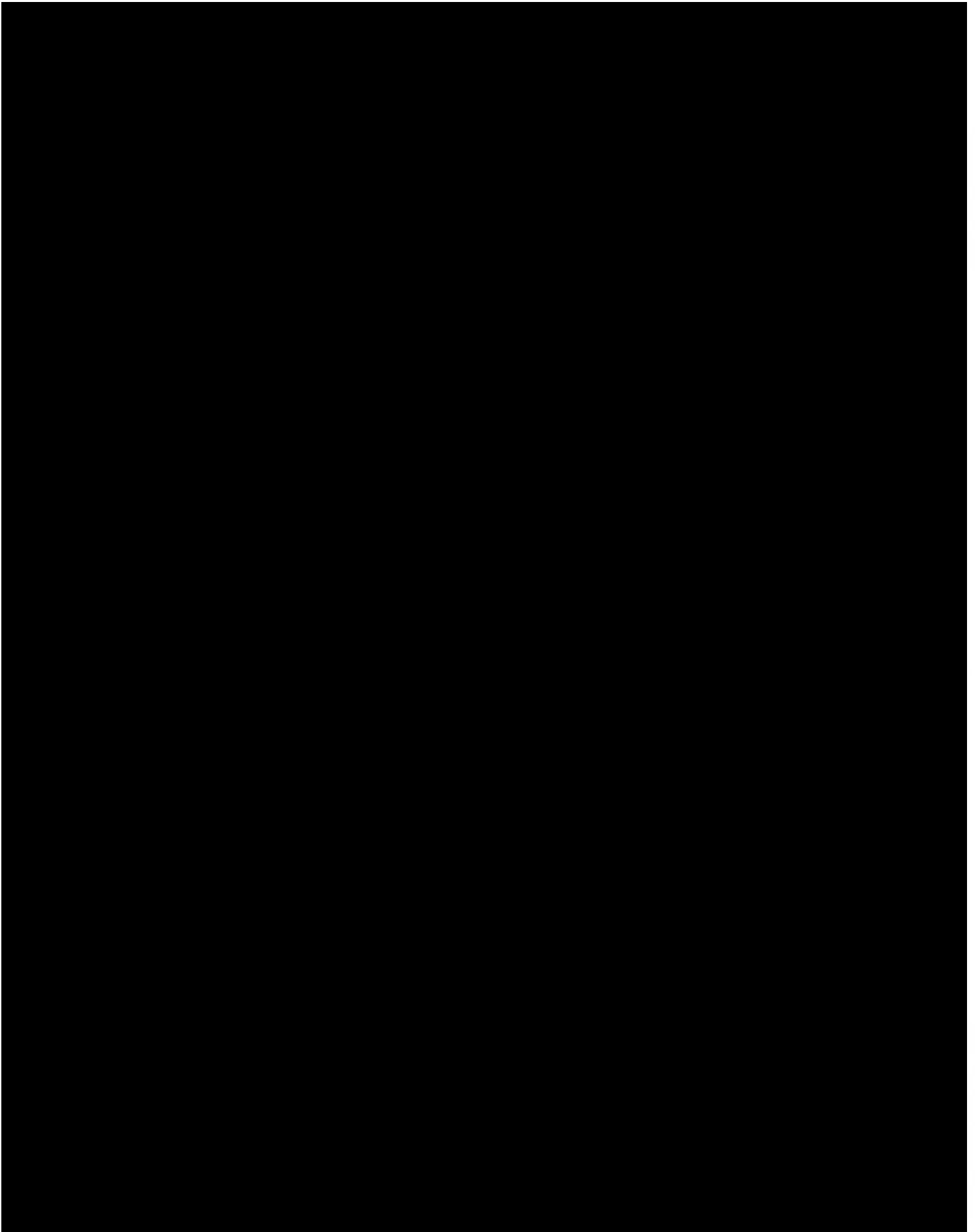
3. For the reasons detailed below, there is probable cause to believe that the Subject Premises contain evidence, fruits, and instrumentalities of violations of: 31 U.S.C. §§ 5314, 5322(a) (failure to file a report of foreign bank and financial accounts); 22 U.S.C. § 611, *et. seq.* (foreign agents registration act); 26 U.S.C. § 7206(1) (filing a false tax return); 18 U.S.C. § 1014 (fraud in connection with the extension of credit); 18 U.S.C. §§ 1341, 1343, and 1349 (mail fraud, wire fraud, and conspiracy to commit these offenses); 18 U.S.C. §§ 1956 and 1957 (money laundering and money laundering conspiracy); 52 U.S.C. §§ 30121(a)(1)(A) and (a)(2) (foreign contribution ban); and 18 U.S.C. §§ 371 and 2 (conspiracy, aiding and abetting, and attempt to commit such offenses) (collectively, the “Subject Offenses”).



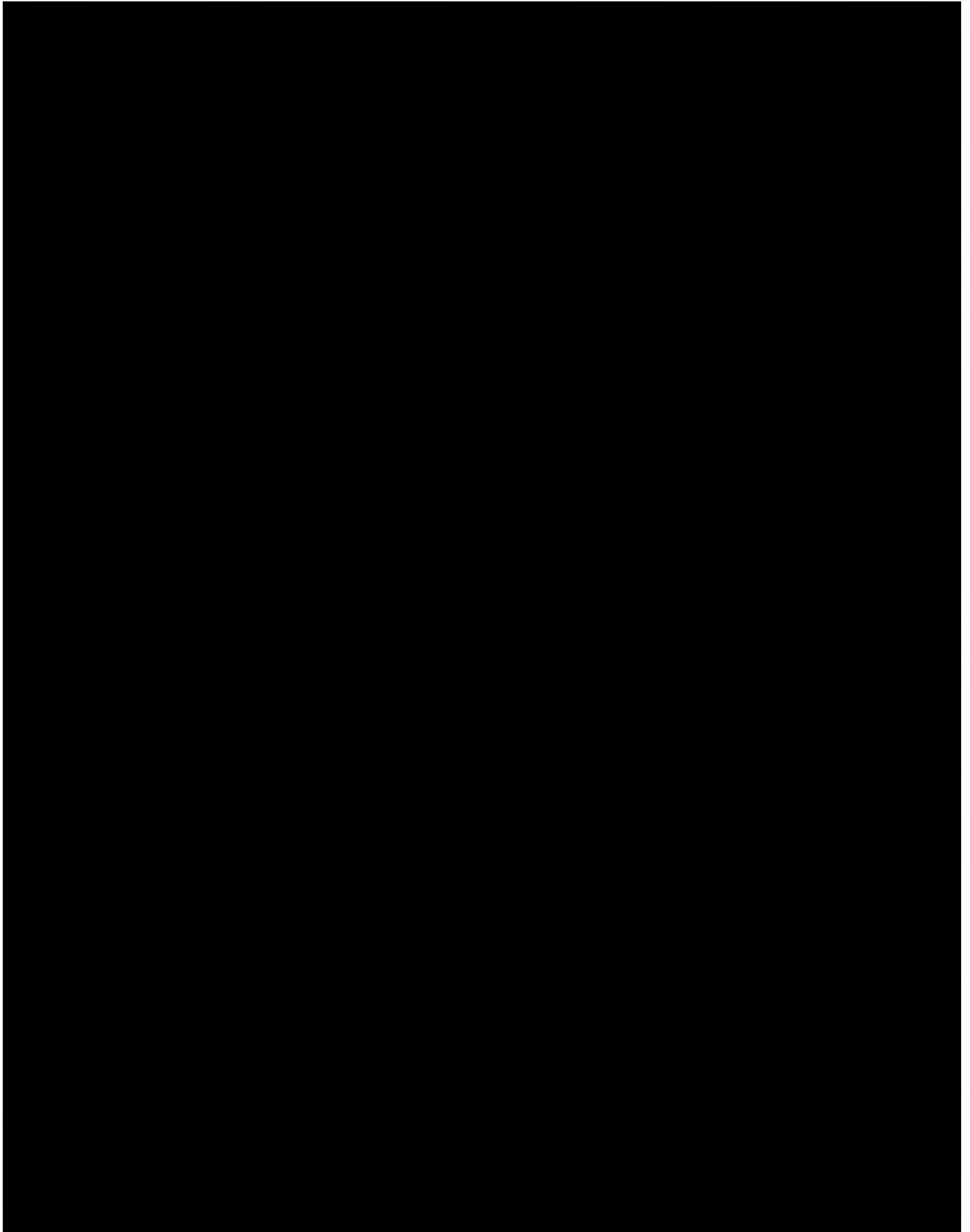




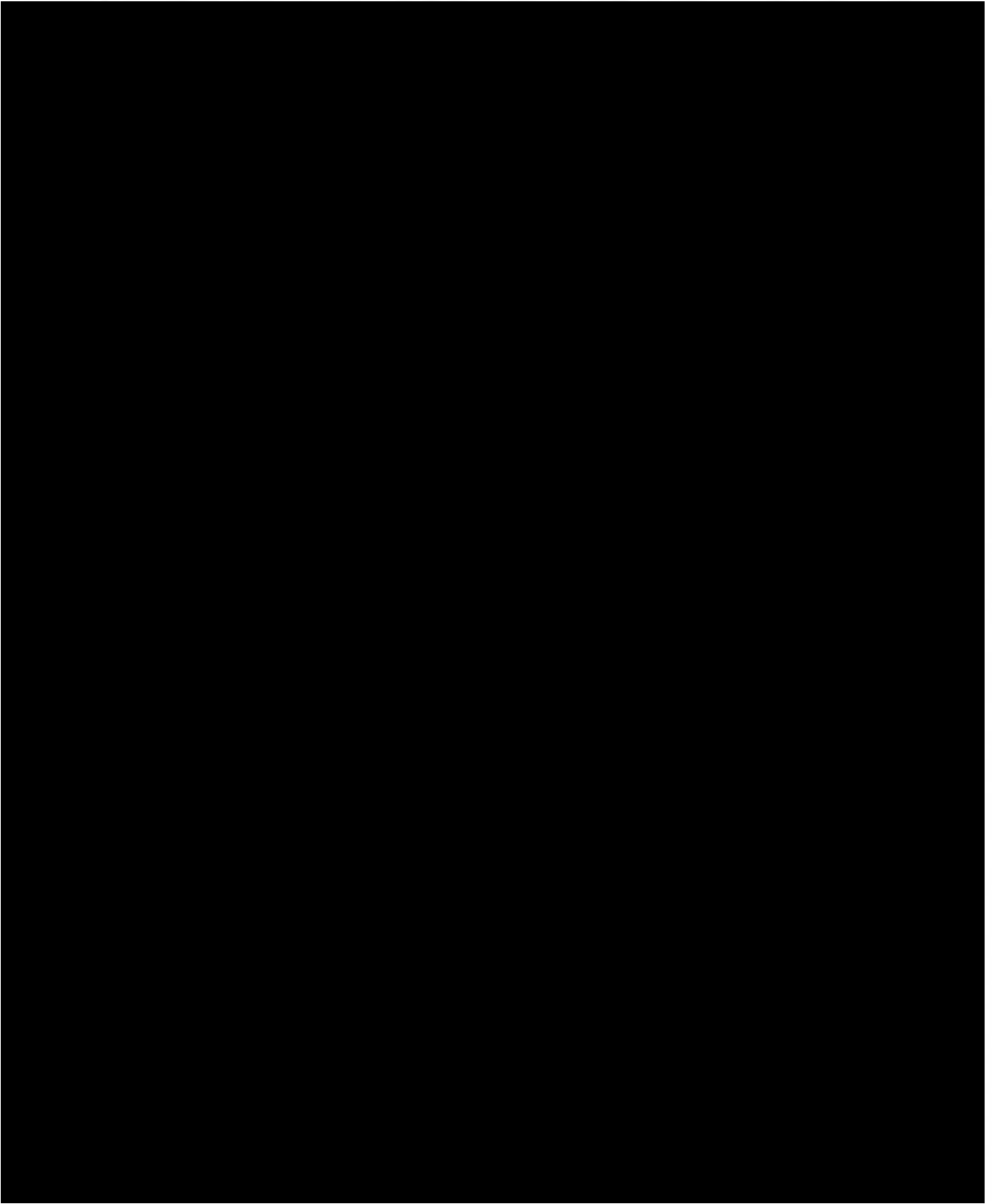


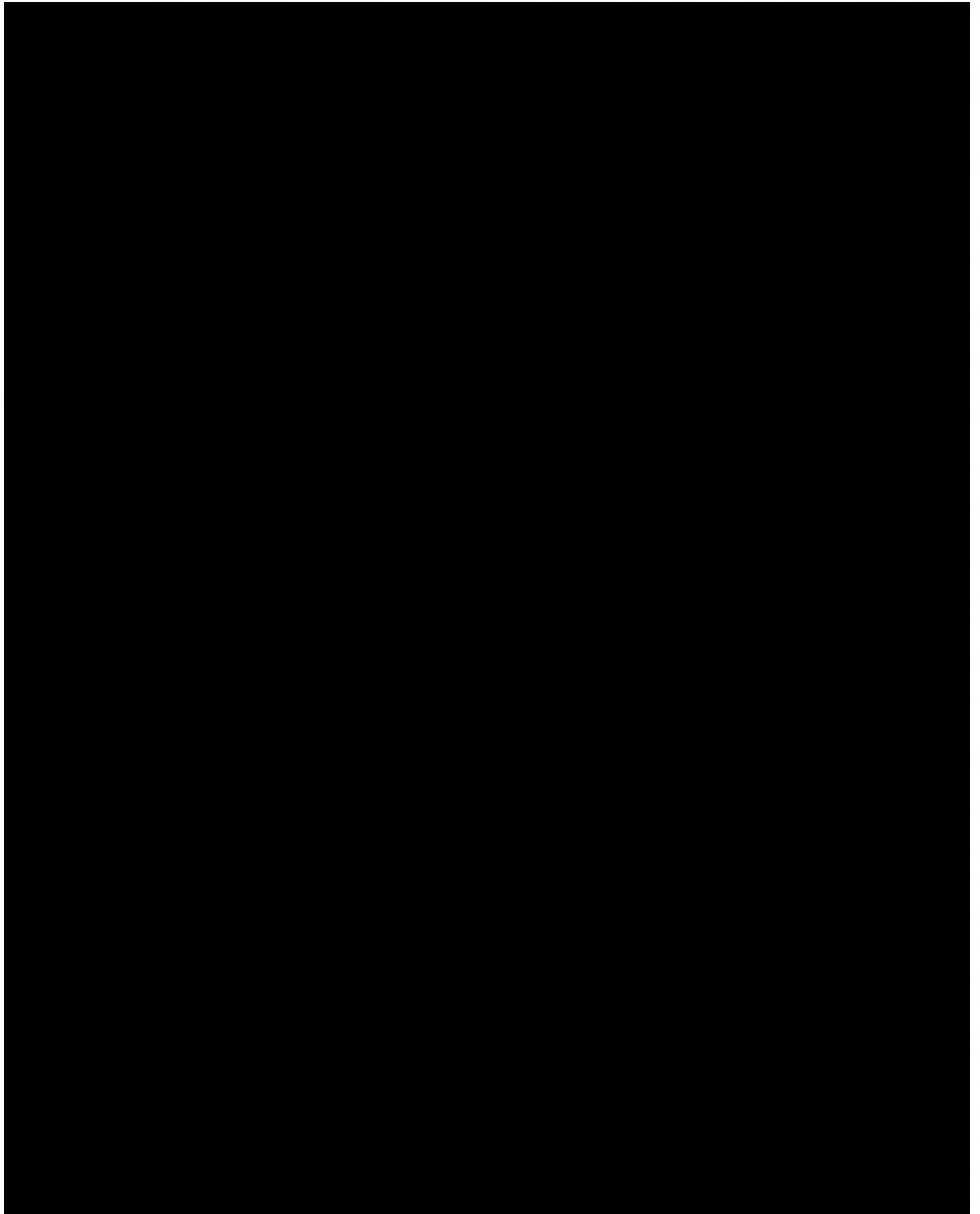


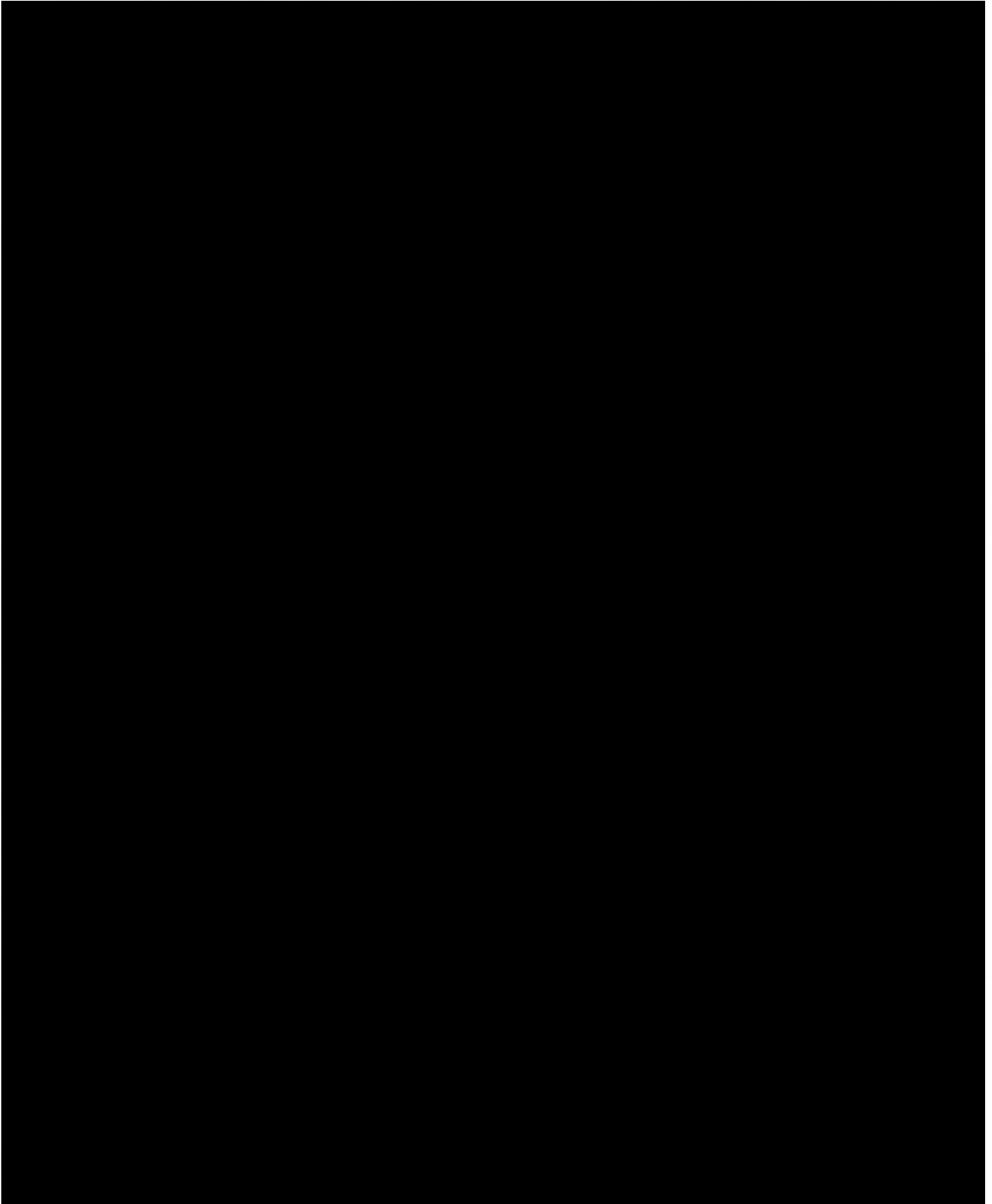


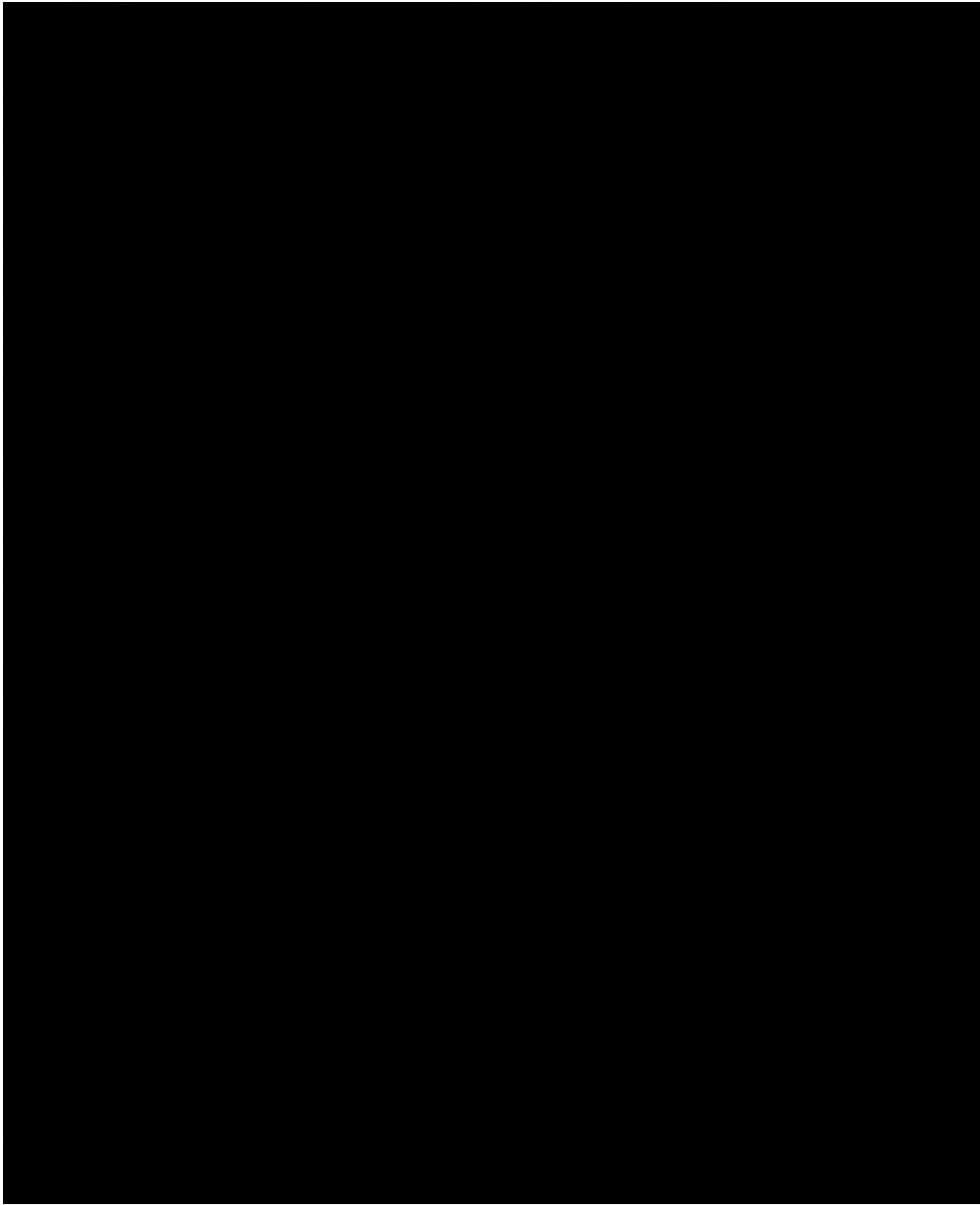


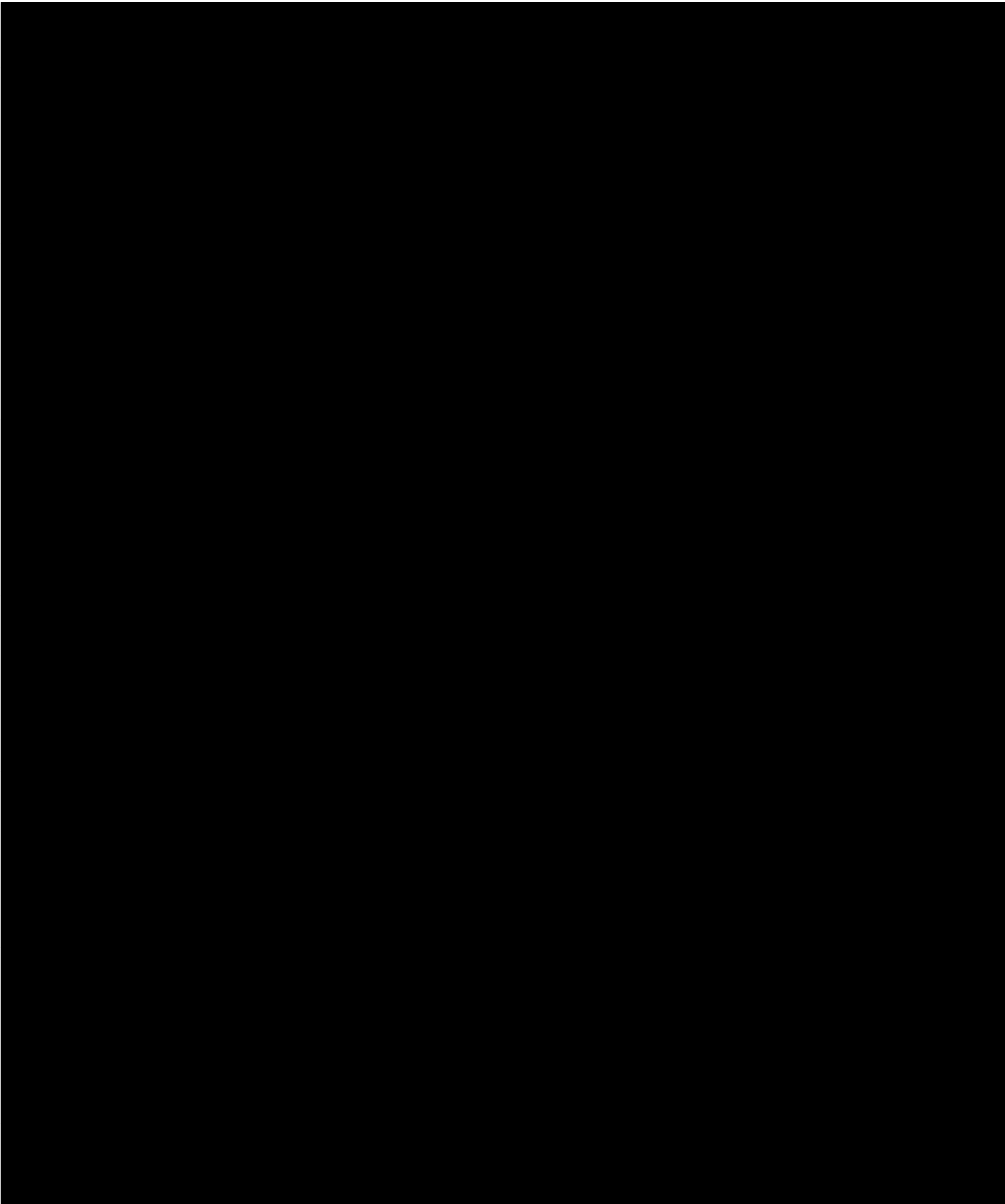


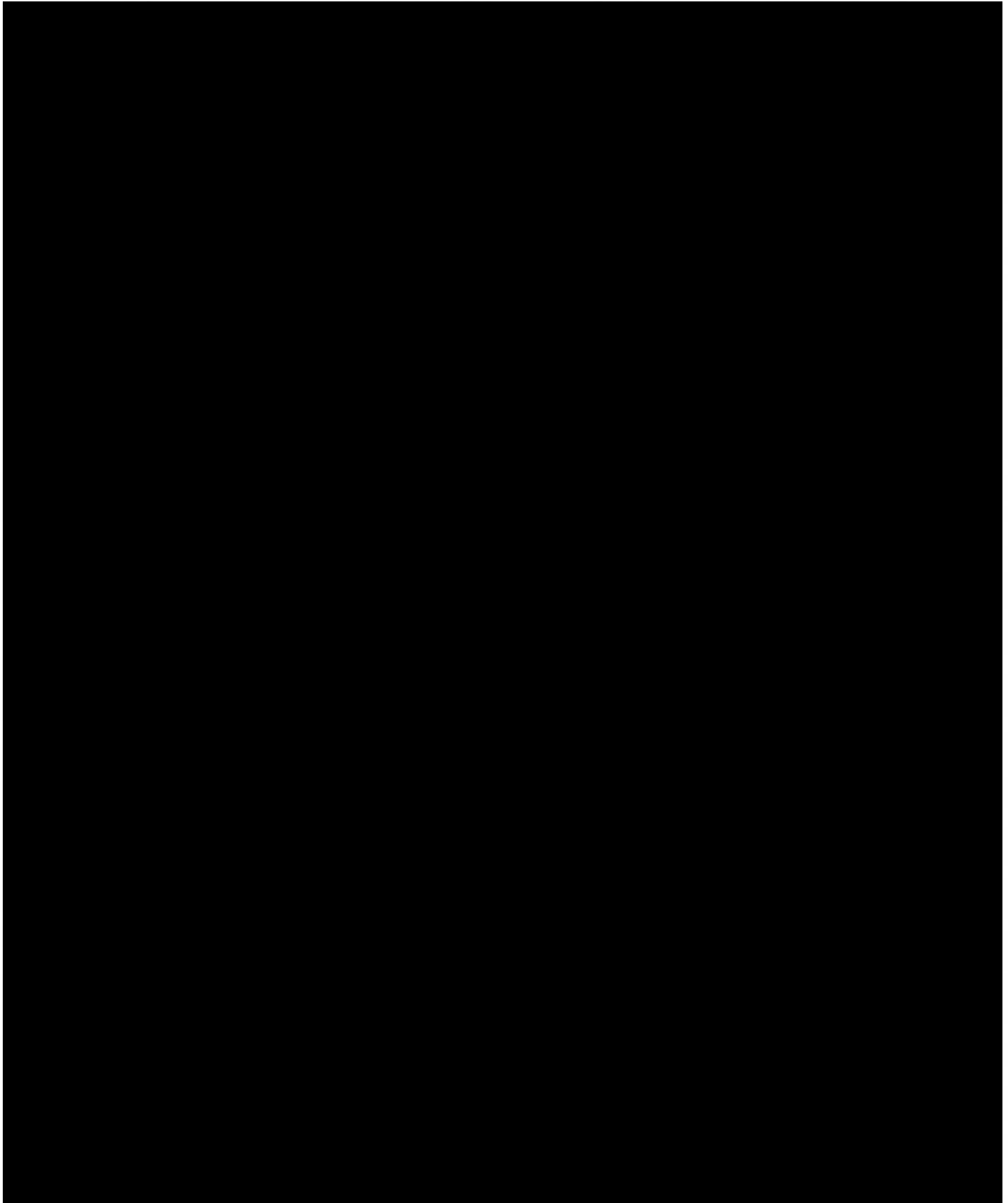




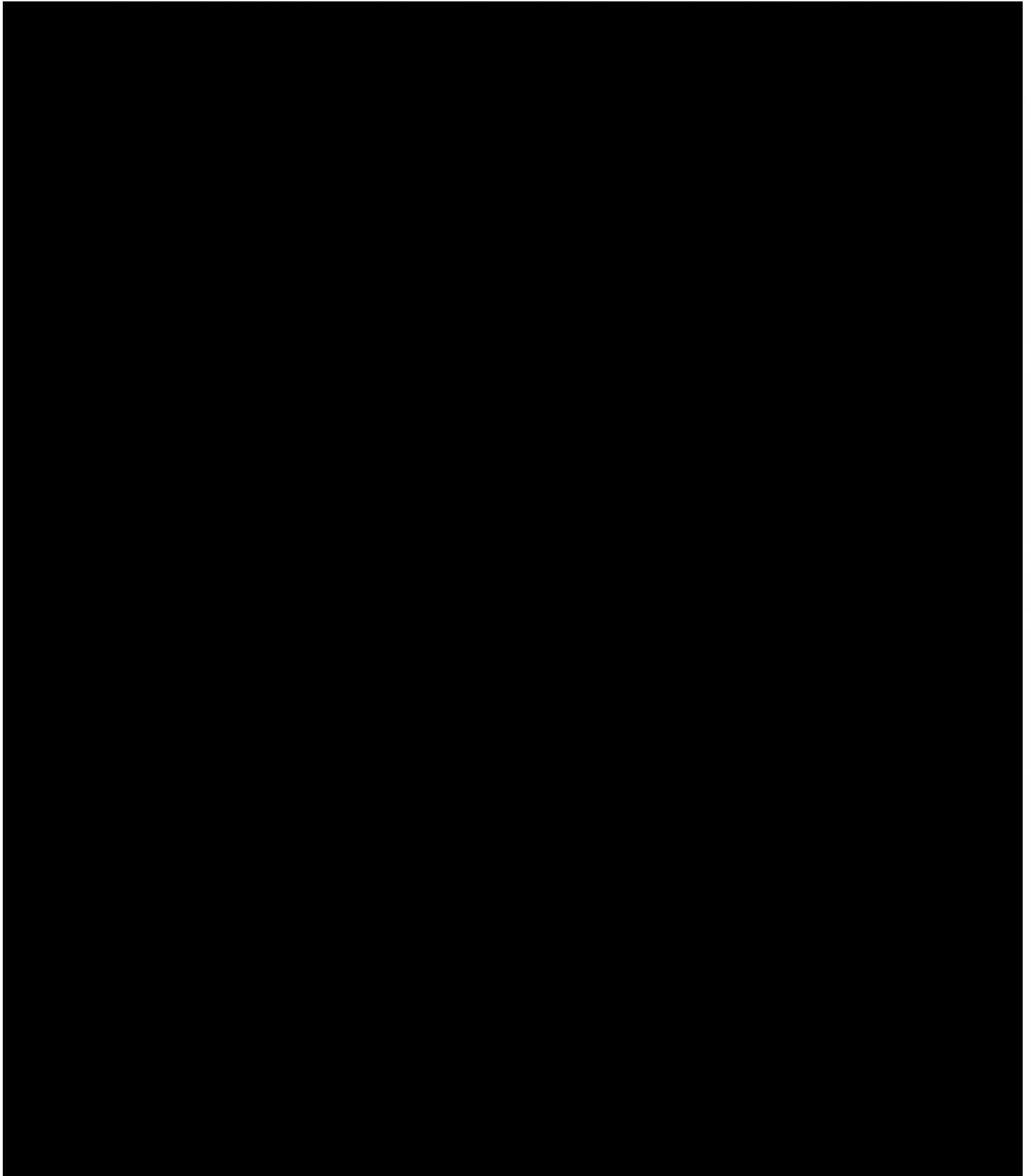


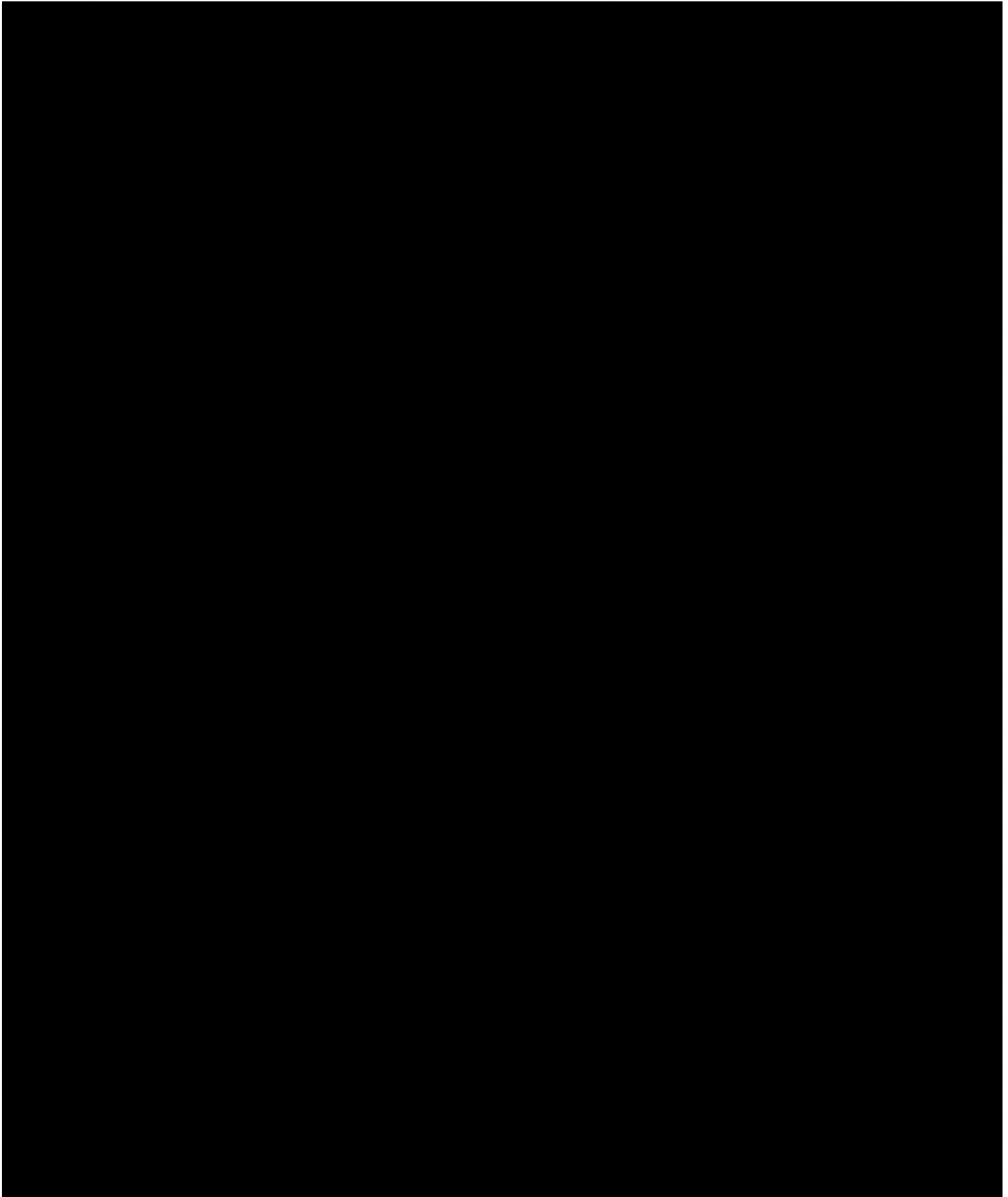


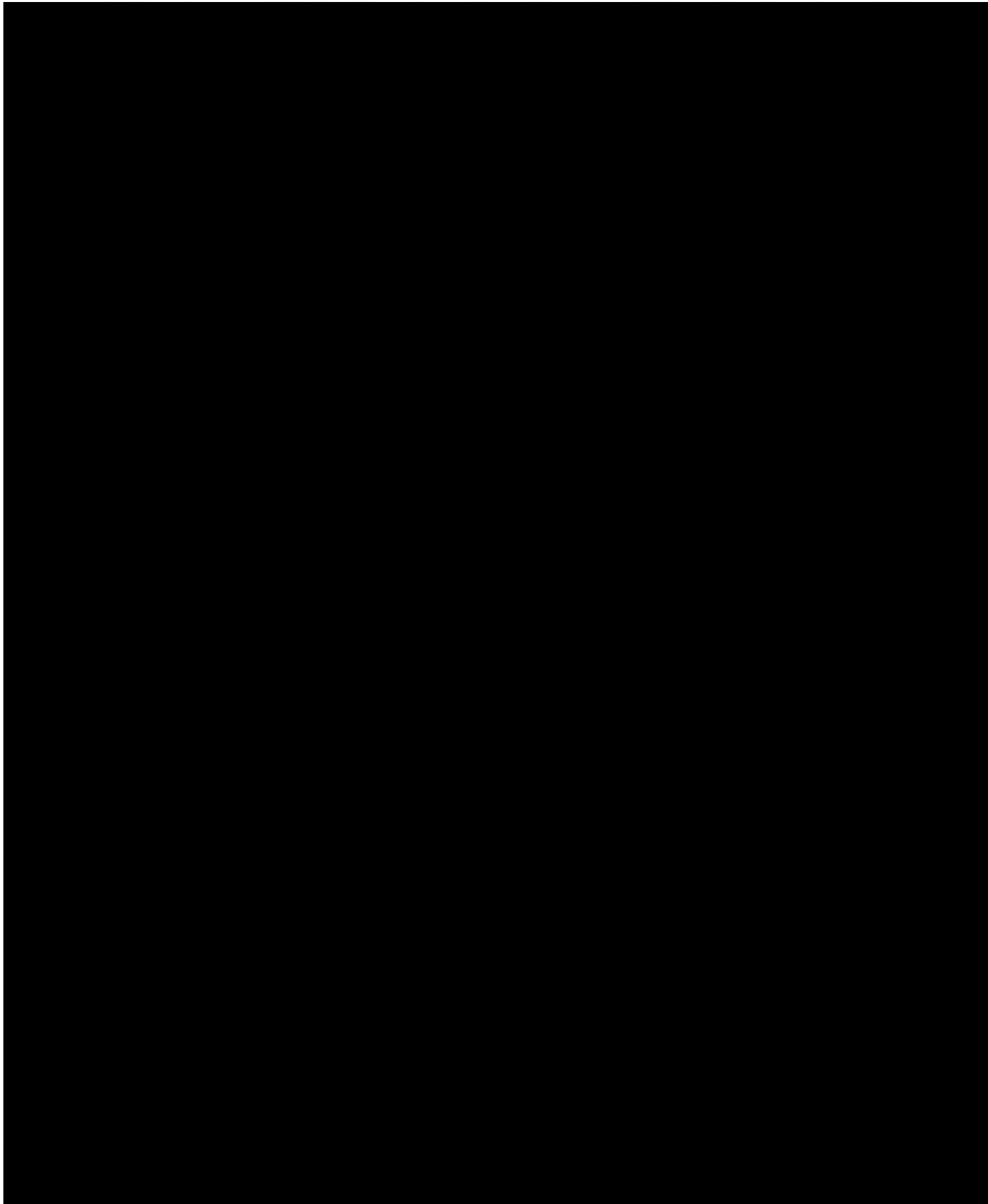


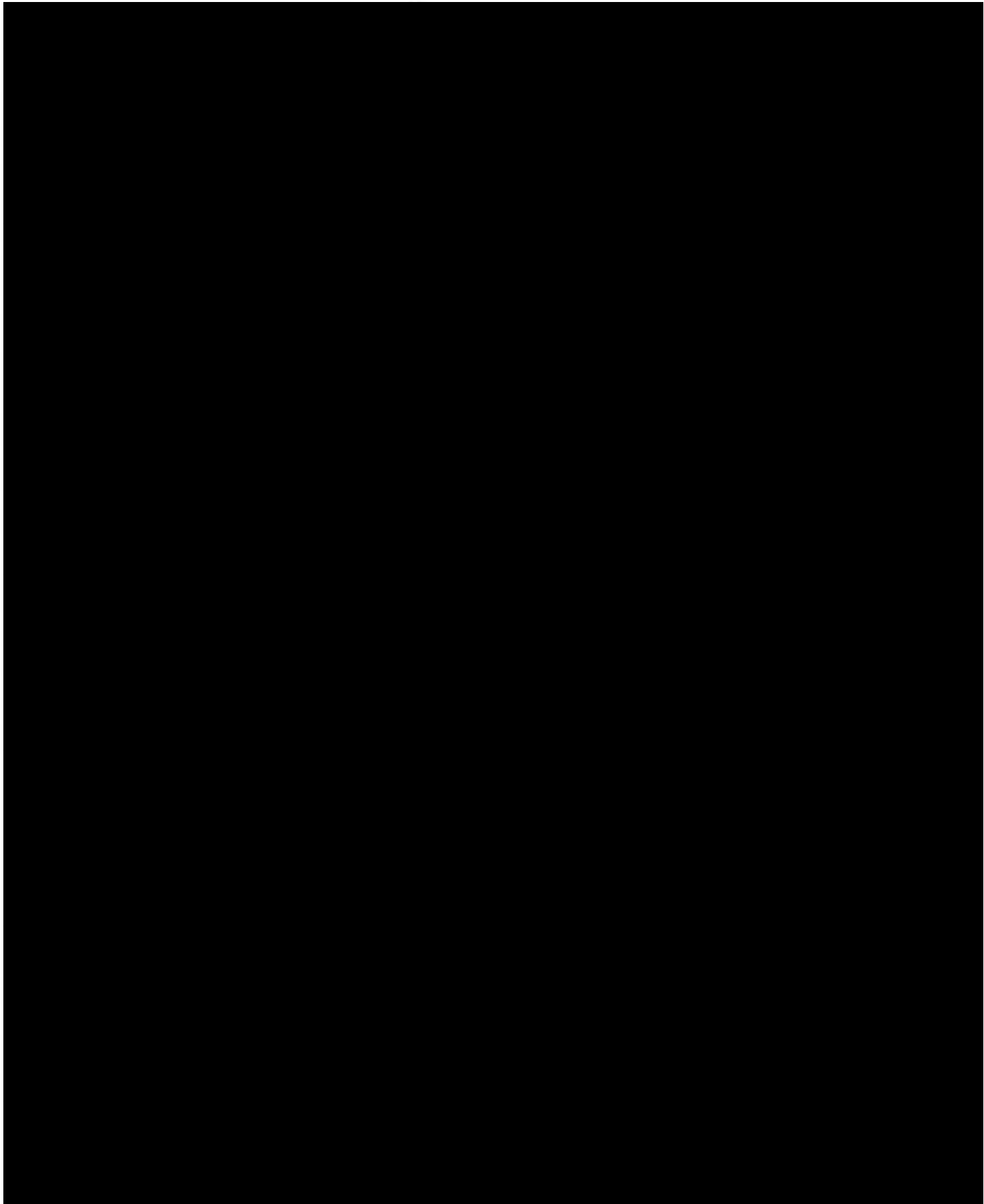


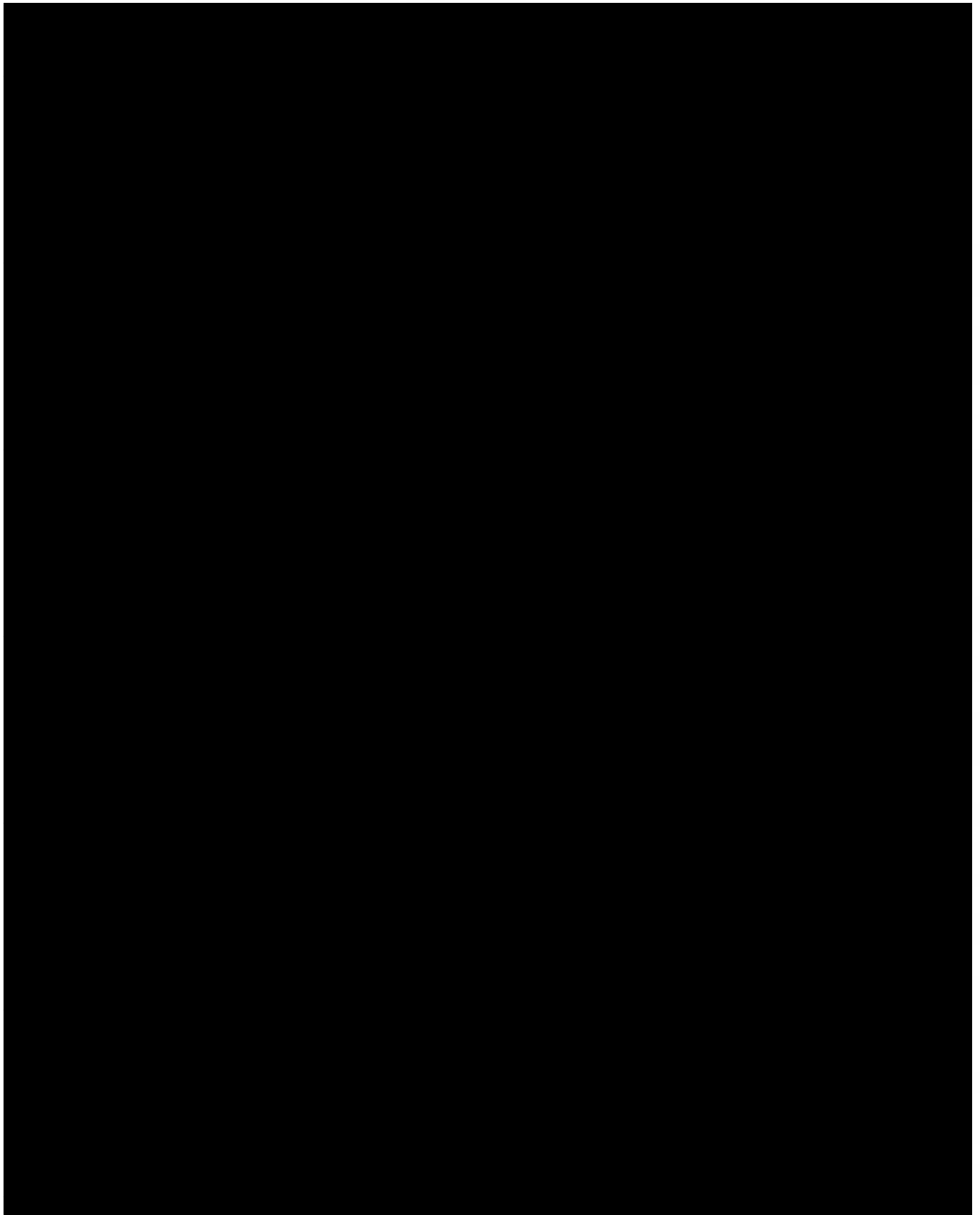


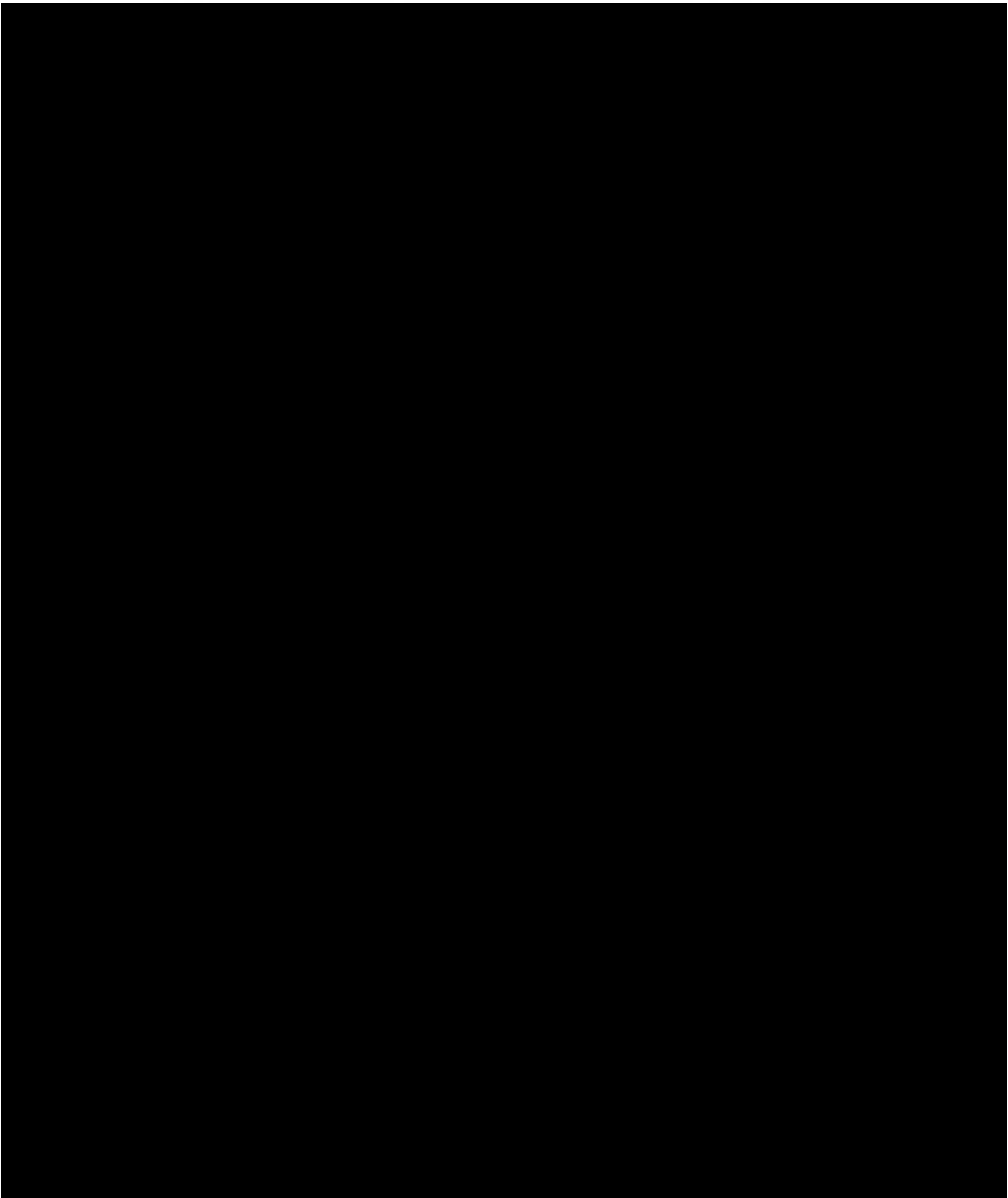


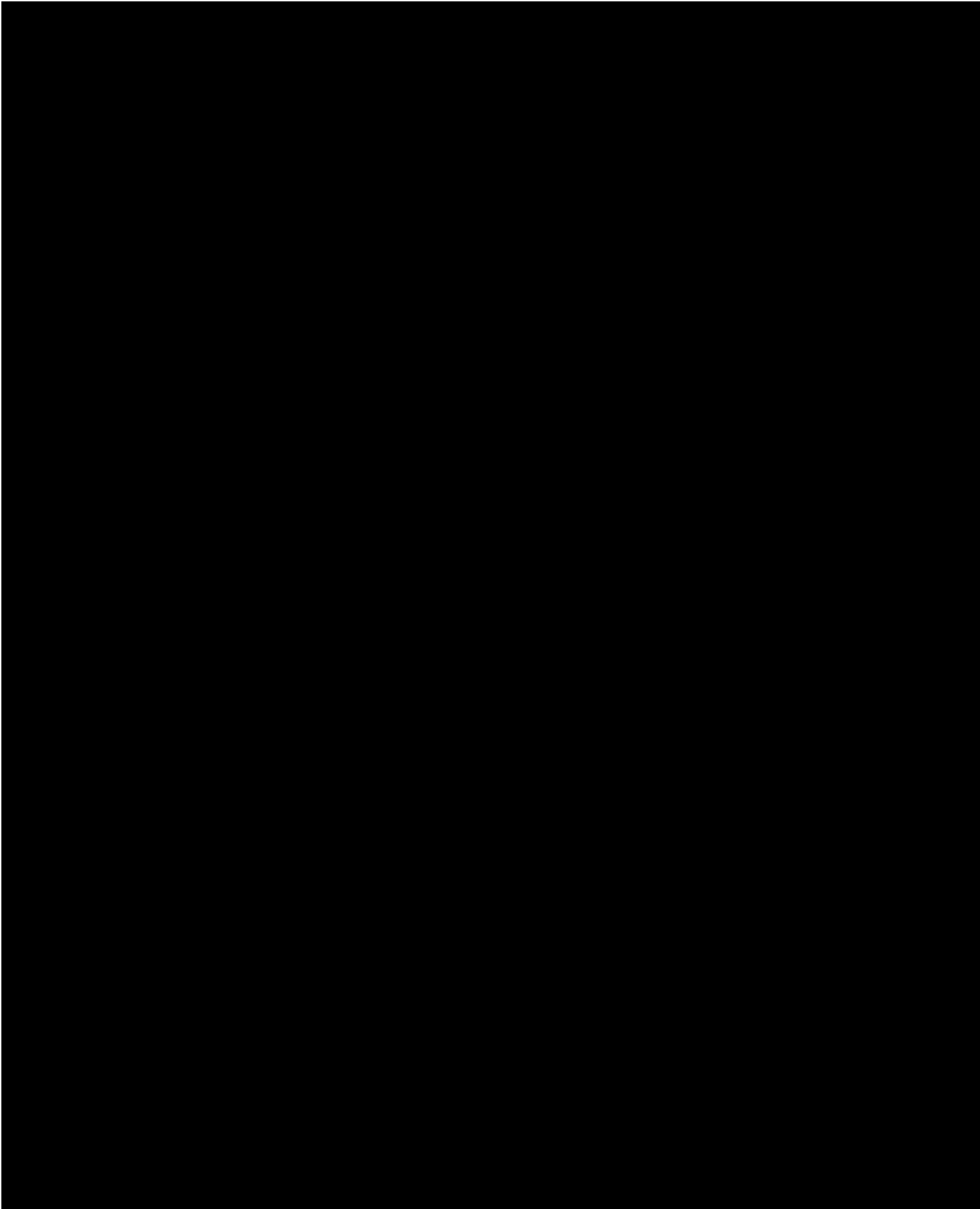


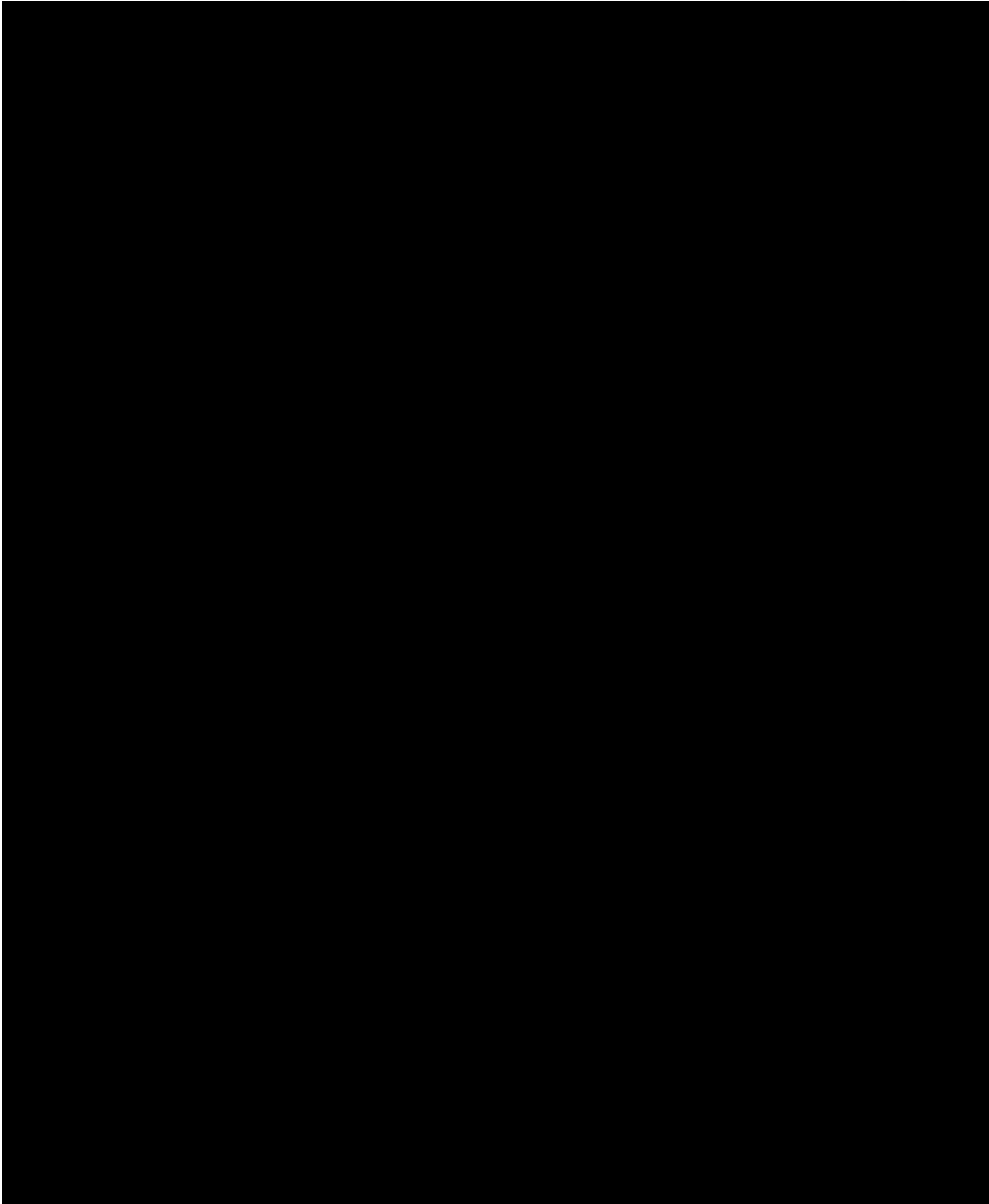




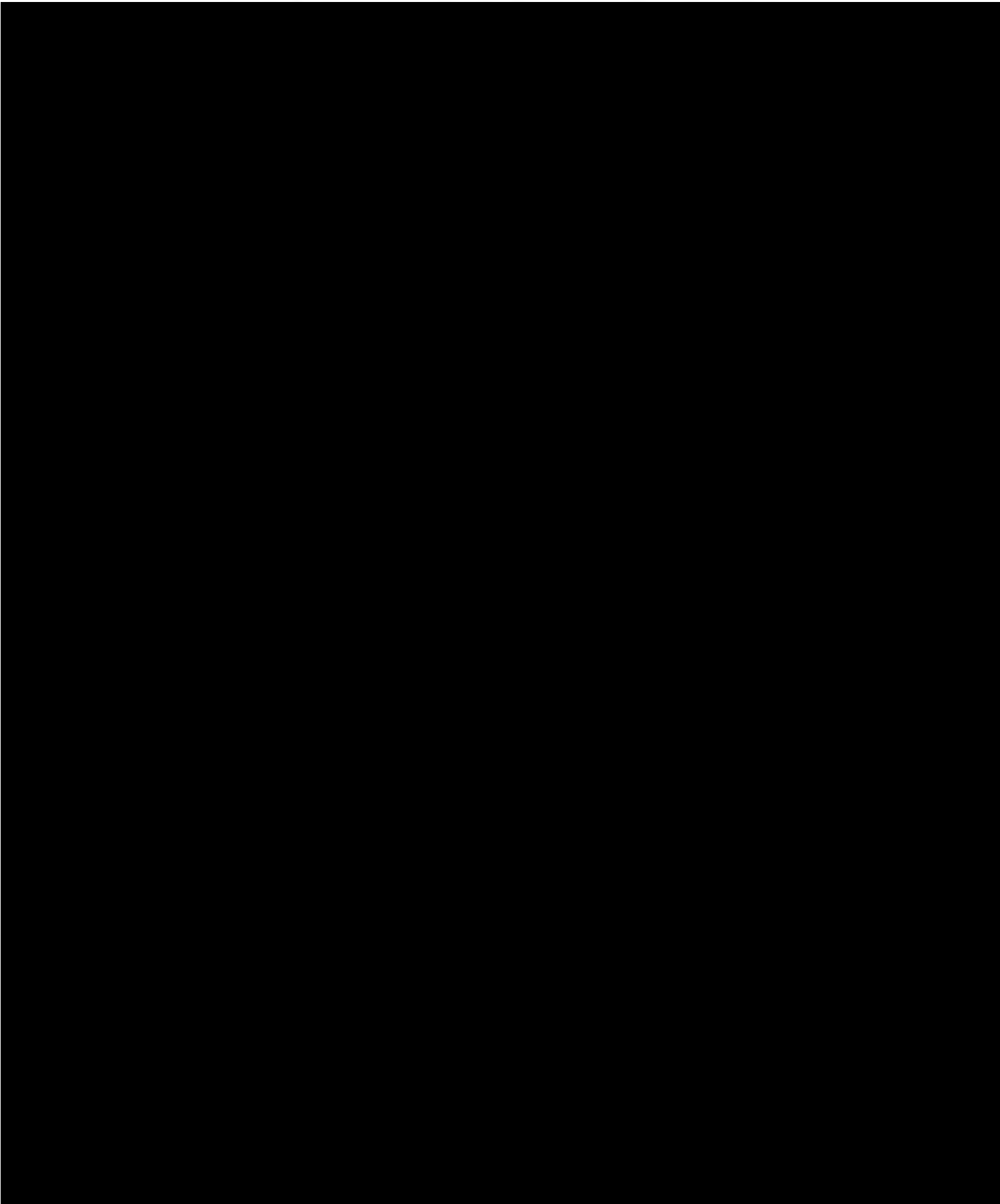


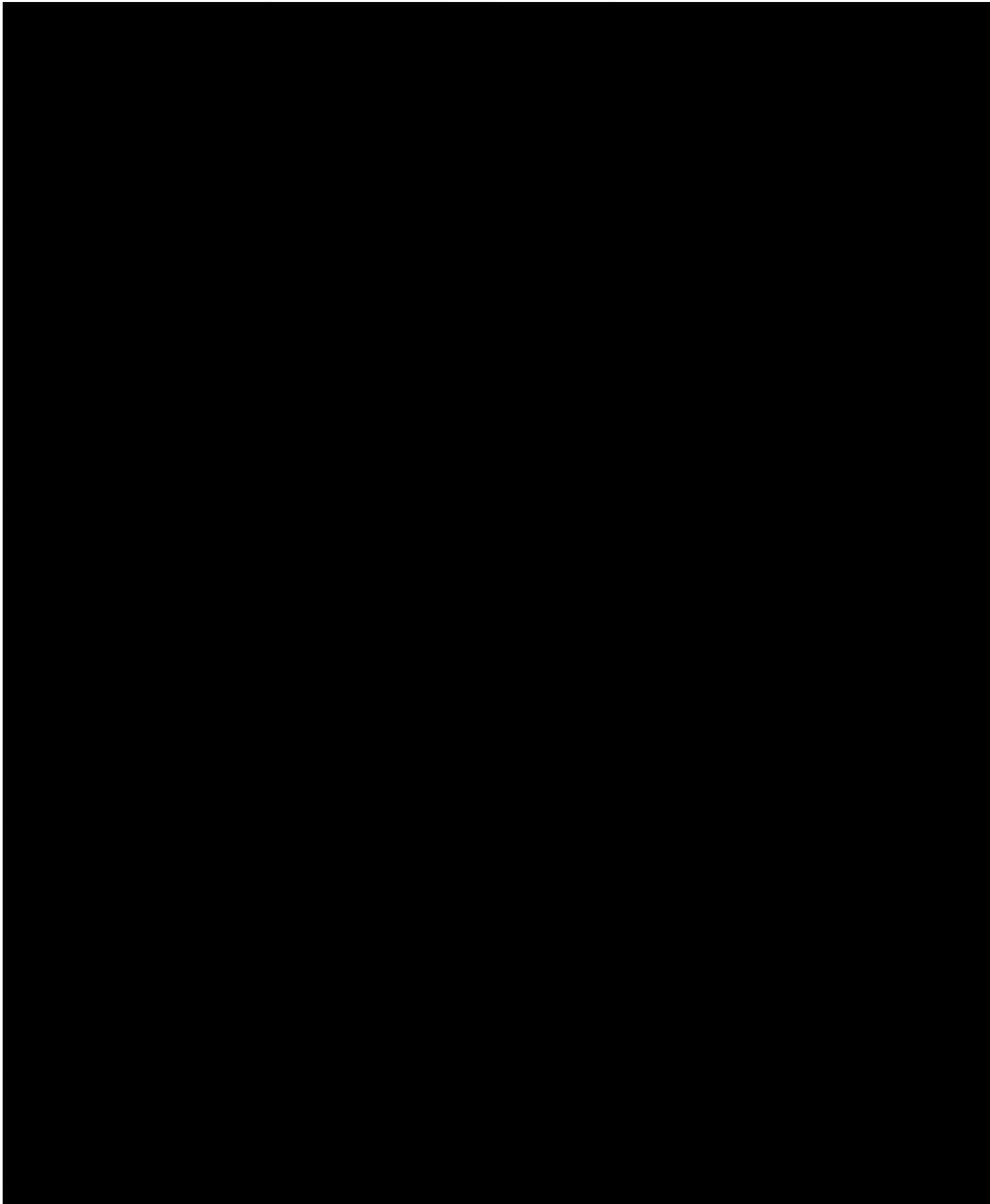


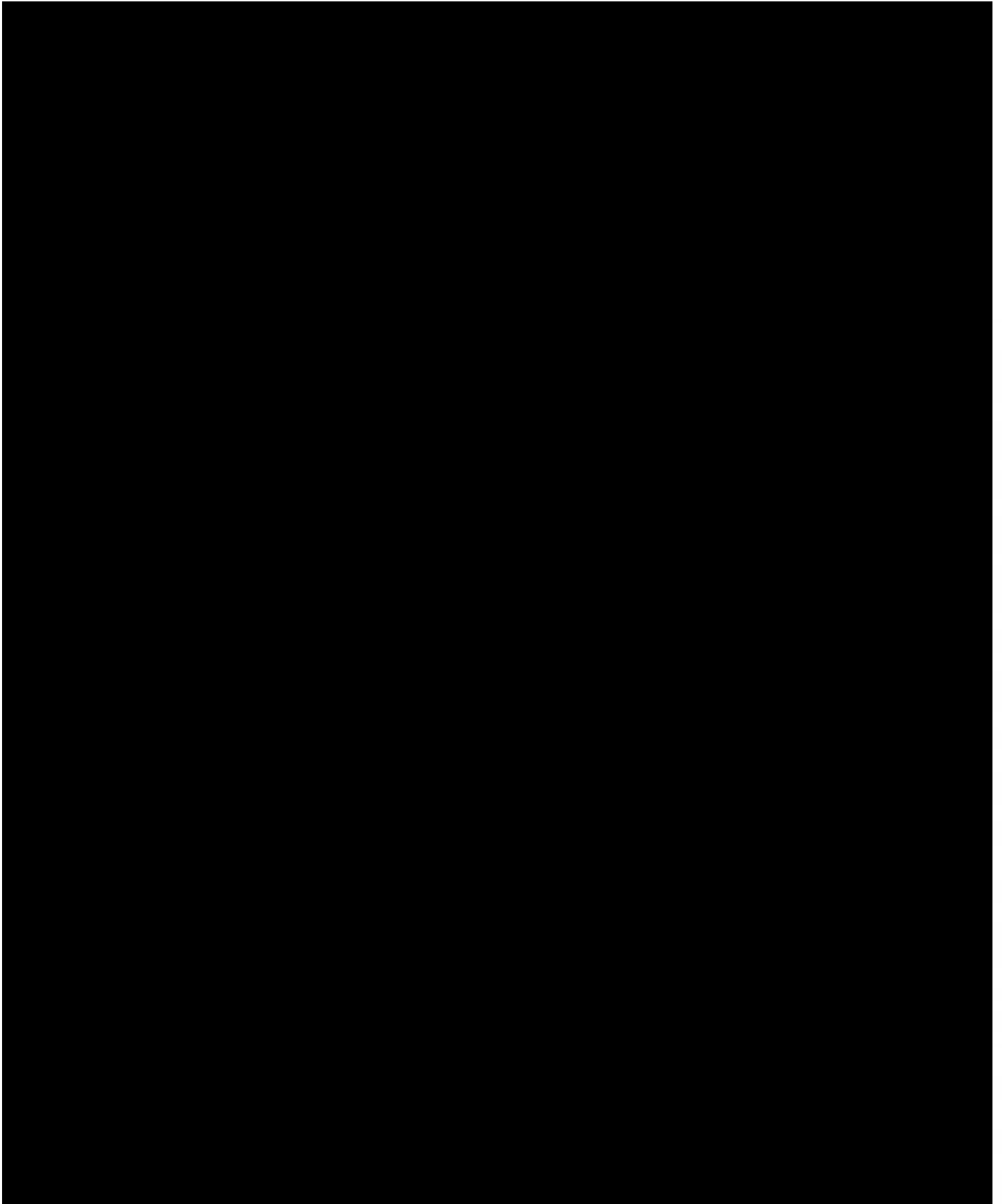


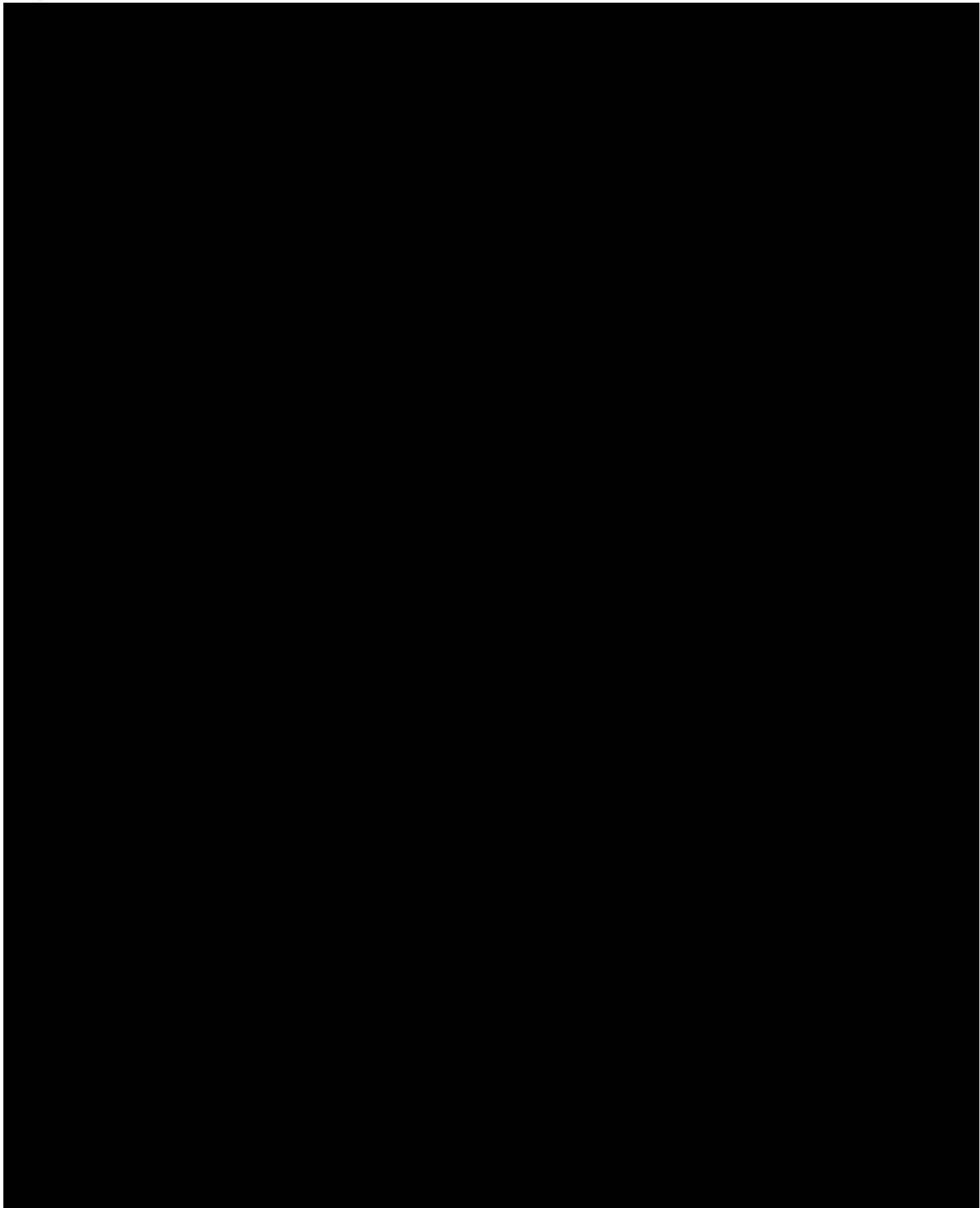


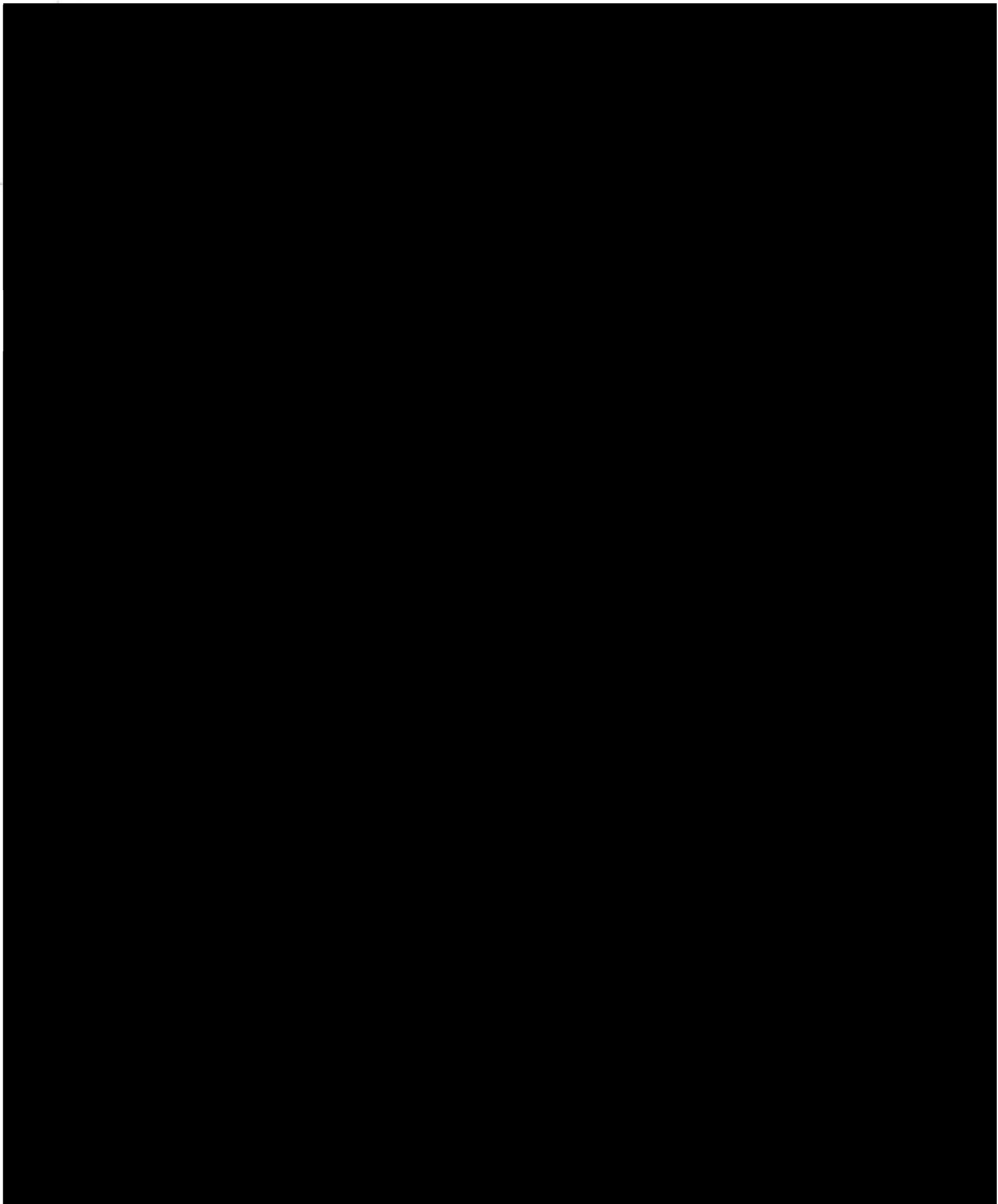


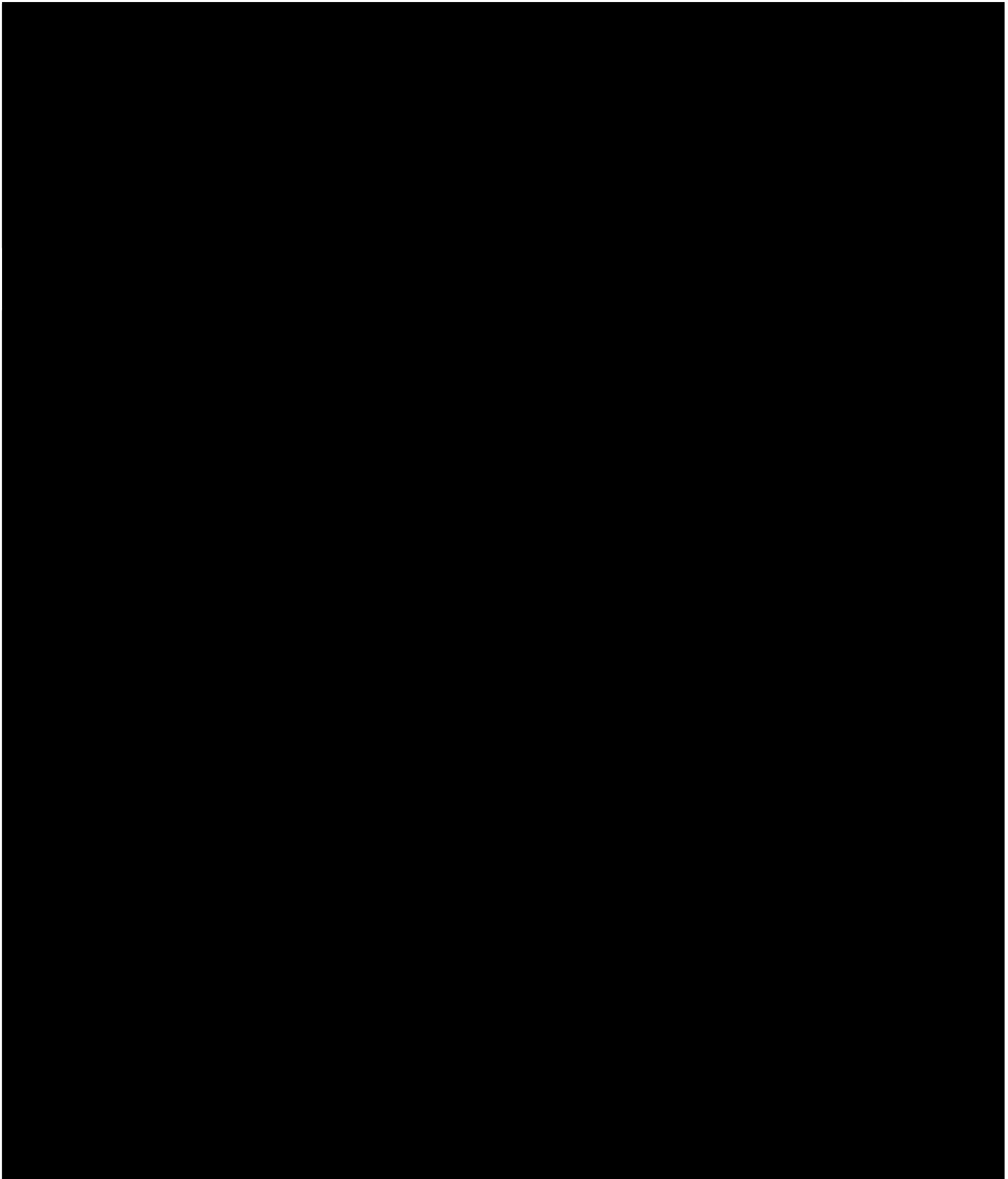


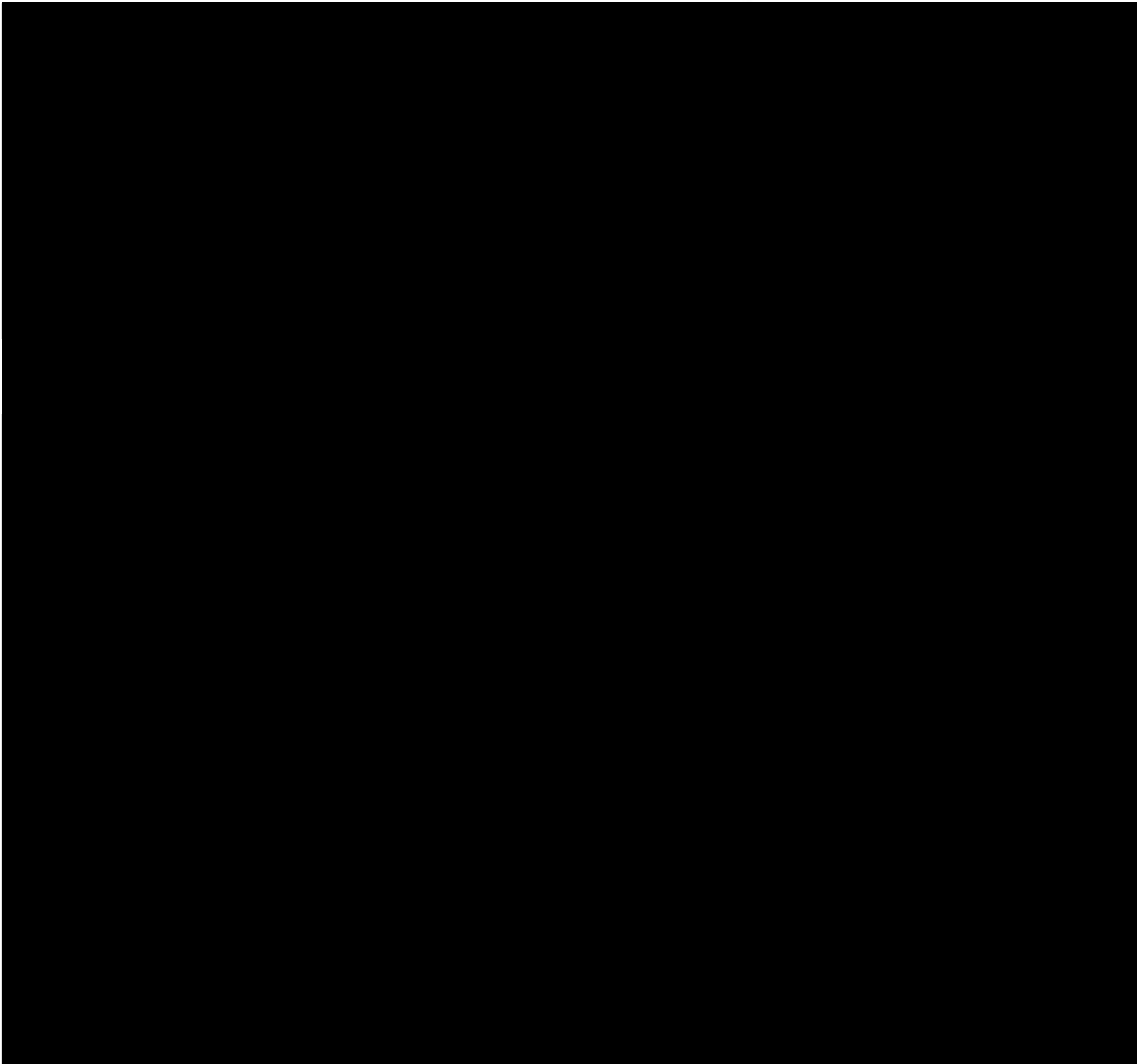












65. [REDACTED] indicated that Manafort used his home to do business and maintained records of his businesses at his home. For instance, some of the material that was moved to [REDACTED] [REDACTED] included files from Manafort's former residence on [REDACTED] in Alexandria, Virginia. [REDACTED] indicated that Manafort was using his former residence as an office at the time. [REDACTED] also advised the FBI that company documentation was being kept at the Subject Premises. In particular, [REDACTED] informed the FBI that in late April or early May of 2017, Kathleen

Manafort told him that she and Manafort were reorganizing their lives and as part of that process were getting documents ready for meetings with their attorney. At the same time, [REDACTED] saw miscellaneous documents on a coffee table at the Subject Premises, including but not limited to Federal Election Commission documents.

66. [REDACTED] also informed the FBI that one of the rooms in the Subject Premises is used as an office, and that [REDACTED] has seen business records in that office, including in one or two drawers. Among the records maintained in the drawers were records related to Manafort's various business entities; including John Hannah LLC (as discussed in Paragraph 16 above) and, he believes, DMP International, LLC.

67. In an interview with the FBI on July 19, 2017, [REDACTED] indicated that the last time he was inside the Subject Premises was on or about July 5, 2017, when he picked up Manafort's mail and shipped a suit to another Manafort residence at Manafort's request; and the last time he was at the Subject Premises was on or about July 11, 2017, when he took Kathleen Manafort to the airport.

68. It is reasonable to believe that business records related to Manafort's work in Ukraine, including historical records, would be maintained among the business files kept at the Subject Premises, including the files kept for use in consulting with counsel. On June 27, 2017, Manafort, Gates, and DMP International, LLC registered under FARA for the years 2012-2014 as a result of their political work in Ukraine, having failed to do so previously. This registration followed a series of communications between Manafort, his counsel, and officials in the United States Department of Justice's National Security Division (which administers the FARA registration process) about the FARA requirements. At least one of these communications, dated September 13, 2016, was directed to Manafort at [REDACTED] in Alexandria, VA,



*i.e.*, the Subject Premises. It is therefore reasonable to believe that records relating to this filing (and thus related to Manafort's failure to file previously) are maintained at the Subject Premises, including records of Manafort's work on behalf of the Party of Regions and payments received from them. Among other things, in the Gates Interview, Gates told the FBI that Manafort and he used "standard English" common law contracts for their Ukrainian work and would invoice the customer for payment.<sup>9</sup>

69. These records are particularly valuable since counsel for Manafort has informed the United States Department of Justice that at least as of November 23, 2016, DMP International, LLC purports to have an "Email Retention Policy" which results in its not retaining "communications beyond thirty days." In spite of its title, the policy purports to cover not just email, but "information that is either stored or shared via electronic mail or instant messaging technologies, and documentation residing on any computer or server." The policy also purports to provide that "[e]ach employee may at its [sic] discretion archive certain electronic information that pertains to the company's business or mission," but the the employee "must do so with the knowledge that all emails, electronic documents and other electronic material shall be deleted from corporate equipment, including but not limited to, computers, servers, and mobile devices, within 30 days of possession of the information."

70. There is also probable cause to believe that the Subject Premises contains records related to Manafort's efforts to secure loans from TFSB on the basis of inconsistent representations about his income and net worth, as described above. Records obtained from TFSB show that in

---

<sup>9</sup> In contrast, in their June 27, 2017, FARA filings, Gates, Manafort, and DMP International, LLC indicated that there was no formal written contract of exchange of correspondence between the parties. In such circumstances, the FARA form requires the filer to "give a complete description" of the terms and conditions of the oral agreement or understanding, its duration, the fees and expenses, if any, to be received." The June 2017 filings provide none of that information.

approximately August 2016, Manafort submitted bank statements for two accounts at Citi to TFSB in connection with his application for lending. One of the two bank statements submitted to TFSB is addressed to Kathleen Manafort at the address of the Subject Premises. Bank records also show that beginning in December 2016, bank statements for the other account were directed to the same address. Accordingly, there is probable cause to believe that bank statements and other documentation related to those accounts, which formed part of the TFSB's consideration of Manafort's request for lending, could be found at the Subject Premises.

71. Additionally, there is probable cause to believe that other financial records relevant to the Subject Offenses will be found at the Subject Premises. Manafort's prior residence in Alexandria, [REDACTED], was listed as the address of record for a number of accounts, including accounts at First Republic Bank in Chicago that were closed in 2014 following anti-money laundering concerns by the bank, as discussed in Paragraph 16 above. From my training and experience, I am aware that individuals and businesses often retain copies of financial records for several years, including in connection with tax filing obligations. Accordingly, and given the fact that Manafort and his wife moved to the Subject Premises from his prior residence in the same city in approximately May of 2015, it is reasonable to believe that financial records sent to his prior residence may be found at the Subject Premises. Additionally, a mail cover conducted by the FBI, involving the review of the outside cover of United States Postal Service (USPS) mail addressed to the Subject Premises, reveals that during the period between approximately June 13, 2017 and July 12, 2017, mail to the Subject Premises included, among other things, a first class mailing from TFSB (the lender described above), mail from M&T Bank, and a statement from American Express addressed to both Paul Manafort and "Davis Manafort Part," which I believe to refer to Davis Manafort Partners.

72. Further, there is probable cause to believe that the Subject Premises contains physical evidence in the form of physical items purchased through the use of funds from foreign bank accounts, including from the Cypriot bank accounts described above. For instance, given that Manafort lives at the premises, there is probable cause to believe that men's clothing and accessories purchased at one or both of the clothing vendors and paid for by wire transfers from various Cyprus accounts, as referenced in Paragraph 14 above, will be found at the Subject premises. Bank records and records obtained from the clothiers show that between 2009 and 2012, Manafort purchased more than approximately \$760,000 in merchandise from these two clothiers using funds wired from several of the Cypriot accounts. Purchases included multiple suits and jackets in excess of \$10,000 and at least one limited edition Bijan Black Titanium "Royal Way" watch, purchased for \$21,000. Between approximately 2009 and spring 2015, invoices for Manafort's purchases from Alan Couture were sent to Manafort's previous Alexandria residence on Mount Vernon Circle; more recently, invoices have been sent to Manafort at the Subject Premises. According to [REDACTED] there are two closets at the Subject Premises that contain clothing and jewelry.

73. There is also reason to believe that rugs purchased with funds from the Cypriot accounts would be found at the Subject Premises. Wire transfers totaling more than \$360,000 were sent from Cypriot accounts directly to J & J Oriental Rugs, a carpet store located in Alexandria, Virginia, near to the Subject Premises. The funds were used to pay for rugs acquired by Manafort. In an interview with the FBI, one of the owners of J & J Oriental Rugs advised that Manafort brought several of his purchases back to the store for cleaning, which remain at the store. It is reasonable to believe that the remaining rugs purchased by Manafort with funds funneled

through the Cypriot accounts will be found at the Subject Premises (to include Premises' storage unit).

74. Although I submit that there is probable cause to seize the aforementioned rugs and clothing as fruits of the Subject Offenses, the FBI does not intend to seize those items. Rather, upon an authorized search of the Subject Premises, the FBI intends to identify and photograph those items.

#### **Computers, Electronic Storage, and Forensic Analysis**

75. As described in Attachment B, this application seeks permission to search for records that might be found on the Subject Premises, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media.<sup>10</sup> Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

76. In a July 2017 interview, ██████ advised the FBI that there is a Mac desktop computer on the desk in the office at the Subject Premises, which is used by Manafort. For a variety of reasons, copies of historical records and current records are also frequently stored on external hard drives, thumb drives, and magnetic disks. There is reasonable cause to believe such media may be contained in and among records of Manafort's business and financial activity at the Subject Premises. FBI interviews of ██████ further confirm that Manafort has made widespread use of electronic media in the course of his business activity. For example, ██████ told the FBI that Manafort had a drawer full of phones and electronic equipment at his old residence in Mount Vernon Square. At one point, Manafort gave ██████ a bag of computers and directed ██████ to

---

<sup>10</sup> A storage medium is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

have the drives wiped before giving them to charity. Manafort also gave [REDACTED] several additional devices, both laptops and cellular phones.

77. I submit that there is probable cause to believe that evidence of the Subject Offenses may be found on storage media located at the Subject Premises, including but not limited to a desktop computer, for at least the following reasons:

- a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet.

Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

- b. Therefore deleted files, or remnants of deleted files, may reside in free space or slack space – that is, in space on the storage medium that is not currently being used by an active file –for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.

- c. Wholly apart from user-generated files, computer storage media – in particular, computers’ internal hard drives – contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system



data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

78. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the Subject Premises because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.
- b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the “who, what, why, when,

where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculcating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and

have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculcate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

- c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves.



Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

- e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

79. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

- a. *The time required for an examination.* As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large

volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

- b. *Technical requirements.* Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Subject Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.
- c. *Variety of forms of electronic media.* Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

80. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.


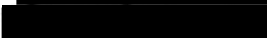
81. Based on the foregoing, I respectfully submit there is probable cause to believe that the Subject Offenses have been committed and that there is probable cause that evidence of the Subject Offenses, as described in Attachment B, is to be found at the Subject Premises.

### III. Conclusion and Ancillary Provisions

82. Based on the foregoing, I respectfully request the Court to issue a warrant to search the Subject Premises, as described in Attachment A to this affidavit, and to seize the items and information specified in Attachment B.

83. In light of the confidential and highly sensitive nature of the continuing investigation, I respectfully request that this affidavit and all papers submitted herewith be maintained under seal until the Court orders otherwise.

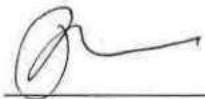
Respectfully submitted,

  
  
Special Agent  
Federal Bureau of Investigation

Sworn to before me on  
July 25, 2017

/s/

Theresa Carroll Buchanan  
United States Magistrate Judge



**ATTACHMENT A**

**The Property to Be Searched**

The premises to be searched (the "Subject Premises") is the condominium unit located at

[REDACTED] Alexandria, VA 22314, including the storage unit numbered [REDACTED]  
[REDACTED] as well as any locked drawers, containers, cabinets, safes, computers, electronic devices, and  
storage media (such as hard disks or other media that can store data) found therein.

**ATTACHMENT B**

**Items to Be Seized (or, in the alternative, identified)**

1. Records relating to violations of 31 U.S.C. §§ 5314, 5322(a) (failure to file a report of foreign bank and financial accounts); 22 U.S.C. § 611, *et. seq.* (foreign agents registration act); 26 U.S.C. § 7206(1) (filing a false tax return); 18 U.S.C. § 1014 (fraud in connection with the extension of credit); 18 U.S.C. §§ 1341, 1343, and 1349 (mail fraud, wire fraud, and conspiracy to commit these offenses); 18 U.S.C. §§ 1956 and 1957 (money laundering and money laundering conspiracy); 52 U.S.C. §§ 30121(a)(1)(A) and (a)(2) (foreign national contributions); and 18 U.S.C. §§ 371 and 2 (conspiracy, aiding and abetting, and attempt to commit such offenses) (collectively, the "Subject Offenses"), occurring on or after January 1, 2006, including but not limited to:

- a. Any and all financial records for Paul Manafort, Jr., Kathleen Manafort, Richard Gates, or companies associated with Paul Manafort, Jr., Kathleen Manafort, or Richard Gates, including but not limited to records relating to any foreign financial accounts and records relating to payments by or on behalf of any foreign government, foreign officials, foreign entities, foreign persons, or foreign principals;
- b. Any and all federal and state tax documentation, including but not limited to personal and business tax returns and all associated schedules for Paul Manafort, Jr., Richard Gates, or companies associated with Manafort or Gates;
- c. Letters, correspondence, emails, or other forms of communications with any foreign financial institution, or any individual acting as the signatory or controlling any foreign bank account;
- d. Records relating to efforts by Manafort, Gates, or their affiliated entities to conduct activities on behalf of, for the benefit of, or at the direction of any foreign government, foreign officials, foreign entities, foreign persons, or foreign principals, including but not limited to the Party of Regions and Viktor Yanukovich;
- e. Records relating to, discussing, or documenting Telmar Investments Limited, Tiakora Ventures Limited, Lucicle Consultants Limited, Actinet Trading Limited, Black Sea View Limited, Bletilla Ventures Limited, Evo Holdings Limited, Global Highway Limited, Leviathan Advisors Limited, Loav Advisors Limited, Peranova Holdings Limited, including but not limited to bank records, canceled checks, money drafts, letters of credit, cashier's checks, safe deposit records, checkbooks, and check stubs, duplicates and copies of checks, deposit items, savings passbooks, wire transfer records, and similar bank and financial account records;
- f. Physical items purchased through the use of funds from Cypriot accounts, including but not limited to rugs purchased from J & J Oriental Rugs, a Bijan Black Titanium "Royal Way" watch, and clothing purchased from House of Bijan and Alan Couture;

- g. Evidence relevant to any false statements, pretenses, representations, or material omissions in connection with communications with the Department of Justice, the Internal Revenue Service, tax preparers, accountants, or banks;
  - h. Communications, records, documents, and other files involving any of the attendees of the June 9, 2016 meeting at Trump tower, as well as Aras and Amin Agalorov;
  - i. Evidence indicating Manafort's state of mind as it relates to the crimes under investigation;
  - j. The identity of any person(s)—including records that help reveal the whereabouts of the person(s)—who communicated with Manafort about any matters relating to activities conducted by Manafort on behalf of, for the benefit of, or at the direction of any foreign government, foreign officials, foreign entities, foreign persons, or foreign principals;
  - k. Any and all daily planners, logs, calendars, or schedule books relating to Manafort or Gates.
2. Computers or storage media used as a means to commit the Subject Offenses.
3. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):
- a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
  - b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
  - c. evidence of the lack of such malicious software;
  - d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;
  - e. evidence indicating the computer user's state of mind as it relates to the crime under investigation;
  - f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;



- g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;
- h. evidence of the times the COMPUTER was used;
- i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
- j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
- k. records of or information about Internet Protocol addresses used by the COMPUTER;
- l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;
- m. contextual information necessary to understand the evidence described in this attachment.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF COLUMBIA

UNITED STATES OF AMERICA,	)	
	)	
v.	)	
	)	Crim. No. 17-201-01 (ABJ)
PAUL J. MANAFORT, JR.,	)	
	)	Judge Amy Berman Jackson
Defendant.	)	

**[Proposed] ORDER**

Upon consideration of Defendant Paul J. Manafort, Jr.'s motion pursuant to Rule 12(b)(3)(C) and Rule 41(h) of the Federal Rules of Criminal Procedure to suppress evidence and all fruits thereof relating to the government's search of his residence located in Alexandria, Virginia (the "Premises"), and any opposition and reply thereto, it is hereby **ORDERED** that the motion is **GRANTED** and it is hereby **FURTHER ORDERED** that all evidence seized from the Premises is hereby **SUPPRESSED**.

**SO ORDERED.**

Dated: \_\_\_\_\_

\_\_\_\_\_  
AMY BERMAN JACKSON  
United States District Judge